



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 Zonebased Policy Firewalls

Alnuman Mohammed Abubaker Altamezwi¹, Abdulwahed Omran E Alalwani², Ashour Alsllami³ ^{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 statefal 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-base d 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).



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022- Available at www.ijraset.com



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.wheras 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.



International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022- Available at www.ijraset.com

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 routs as the main routing configuration.
- 4) Implementing the CBAC and ZBF to provide security firewall to the network.







ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022- Available at www.ijraset.com

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.

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

Table 1 The main devices used to design the sample network

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

R1	Serial4/0 to R2 Seria	al4/1 Capturing from Sta	andard input - Wireshark					
le	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Sta	tistics Telephony <u>T</u> ools	<u>H</u> elp				
K I) 🔍 🗢 🔿 孩	业 🔳 🛢	⊕		🖭 🕁 🖻	1 🍢 🐝 🛱
lter	:			 Expression 	Clea	r Apply		
	Time	Source	Destination	Protocol	Info		10.000	
	26 23.857649	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	27 23.873249	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	28 23.920049	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	29 23.935649	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	30 23.982450	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	31 23.998050	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	32 24.044850	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	33 24.060450	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	34 24.107250	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	35 24.122850	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	36 24.169650	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	37 24.185250	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	38 24.232050	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
	39 24.247650	20.20.20.2	192.168.100.3	ICMP	Echo	(ping)	reply	
	40 24.294450	192.168.100.3	20.20.20.2	ICMP	Echo	(ping)	request	
							III	
-	amo 1 : 252 hu	tos on wire (281	6 hitc) 252 hotos	conturod (2916 h	itc)		
Ci	ame I. 552 by	ces on whe (281	o bits), 352 bytes	captured (2010 0	its)		
Ci	sco Discovery	Protocol						

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

	R1 Seri	1 Serial4/0 to R2 Serial4/1 Capturing from Standard input - Wireshark																	
Eile	<u>E</u> di	t <u>V</u> iew	/ <u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	Statistic	s Telep	hony	Tools	<u>H</u> elp									
		۱ 🌢	t 💓		×2	810	2, 4	⇒ •	3	业 🔳 🛢	Ð,	Q	0 🗂	M 1	2 🔼 🕺	2 🛱			
Filt	er:									 Expression. 	Clea	r Ap	ply						
No.		Time		Source			Destina	tion		Protocol	Info								
	339	350.4	447641	192.16	8.50.2		192.1	68.2	00.3	TCP	51474	l > t	elnet	[ACK]	Seq=61	Ack=163	Win=3966	Len=0	
	340	350.4	47641	192.16	8.50.2		192.1	68.2	00.3	TELNET	Telne	et Da	ata						
	341	350.4	178841	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
	342	350.4	178841	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
	343	350.	588042	192.16	8.50.2		192.1	68.2	00.3	TCP	51474	1 > t	elnet	[ACK]	Seq=63	Ack=169	Win=3960	Len=0	
	344	350.6	519242	192.16	8.50.2		192.1	68.2	00.3	TELNET	Telne	et Da	ata						
	345	350.0	550442	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
	346	350.0	550442	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
	347	350.7	744042	192.16	8.50.2		192.1	68.2	00.3	TELNET	Telne	t Da	ata						
	348	350.7	759642	192.16	8.50.2		192.1	68.2	00.3	TCP	51474	1 > t	elnet	[ACK]	Seq=67	Ack=175	Win=3954	Len=0	
	349	350.7	790842	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
	350	350.7	790842	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
	351	350.9	900042	192.16	8.50.2		192.1	68.2	00.3	TCP	51474	l > t	elnet	[ACK]	Seq=67	Ack=181	Win=3948	Len=0	
	352	350.9	978042	192.16	8.50.2		192.1	68.2	00.3	TELNET	Telne	et Da	ata						
	353	351.0	009242	192.16	8.200.3	3	192.1	68.5	0.2	TELNET	Telne	et Da	ata						
٠ [III					
•	rame	1: 3	352 by	tes on	wire (2816 b	its).	352	bytes	captured (2	816 b	its)							
· ·	cisco	HDLO							.,			,							
•	cisco	Disc	overy	Protoc	:01														



Volume 10 Issue VI June 2022- Available at www.ijraset.com

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.

R 3	I3 Serial4/1 to R2 Serial4/0 Capturing from Standard input - Wireshark																	
Eile	Edit	<u>V</u> iew	Go	Capture A	nalyze	Statistics	s Telep	hon <u>y T</u> ools	Hel	р								
D.		<u>e</u> i ei	2		XR	8 0	2, 4	🔿 🖓 😚	⊉		⊕ (a Q	++	¥ (2 🖪 🖇	6 🛱		
Filter	:								•	Expression.	Clear	Apply						
о.		Time		Source			Destinat	ion		Protocol	Info							
	14	3.868	807	192.168	. 50. 2		20.20.	20.1		TELNET	Telnet	t Data						
	15	3.884	407	20.20.20	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	16	3.884	407	20.20.20	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	17	3.931	207	192.168	. 50. 2		20.20.	20.1		TCP	20224	> tel	net	[ACK]	Seq=9	Ack=25	Win=3974	Len=0
	18	4.009	207	192.168	. 50.2		20.20.	20.1		TELNET	Telnet	t Data						
	19	4.024	807	20.20.2	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	20	4.024	807	20.20.20	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	21	4.087	207	192.168	. 50. 2		20.20.	20.1		TCP	20224	> tel	net	[ACK]	Seq=11	Ack=31	Win=3968	Len=0
	22	4.180	808	192.168	. 50.2		20.20.	20.1		TELNET	Telnet	t Data						
	23	4.196	408	20.20.20	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	24	4.196	408	20.20.20	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	25	4.274	408	192.168	. 50. 2		20.20.	20.1		TCP	20224	> tel	net	[ACK]	Seq=13	3 Ack=37	Win=3962	Len=0
	26	4.368	800	192.168	. 50. 2		20.20.	20.1		TELNET	Telnet	t Data						
	27	4.383	608	20.20.2	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
	28	4.383	608	20.20.20	0.1		192.10	58.50.2		TELNET	Telnet	t Data						
														III				
F	ame	1: 2	4 by	tes on wi	re (1	92 bits	5), 24	bytes ca	ptur	ed (192	bits)							
C	isco	HDLC	- ,															
C	isco	SLAR	P															

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.

3 R4 Serial4/0 to R3 Serial4/0 Capturing from Standard input - Wireshark									
File Edit View Go Capture Analyze Sta	atistics Telephony <u>T</u> ools <u>H</u> e	<u>H</u> elp							
] (▙▕▕█▎▆▕▝ቒ、ቒ、፼、▎▌▏▓▏ᢂ▕ॺ▖▓▖▏▓							
Filter:	•	 Expression Clear Apply 							
No. Time Source	Destination	Protocol Info							
1444 8414.21399 N/A	N/A	SLARP LINE REEPAIIVE, 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)							
1450 9424 10762 N /A	NI / A	ELABB Line koonaliyo outooina coquence 97 naturned coquence 20							
•		m							
Frame 1: 24 bytes on wire (192	bits), 24 bytes captur	ured (192 bits)							
Cisco HDLC									
Cisco SLARP									

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



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022- Available at www.ijraset.com

R3 Se	rial4/1 to	R2 Serial4/0 Cap	oturing from	m Standard i	nput - Wire	eshark														
<u>File</u>	lit <u>V</u> iew	<u>G</u> o <u>C</u> apture	<u>A</u> nalyze	Statistics	Telephony	<u>y T</u> ools	Help	0												
	۵ 🌢	i 🗟 🖻 🖥	XZ		\$	4	₹		Ð,	ର୍ଷ୍	••••••••••••••••••••••••••••••••••••••	¥	1 8 %							
Filter:							•	Expression	Clea	r Apply										
0.	Time	Source		D	estination			Protocol	Info											
105	9019.	51053 50. 50	. 50.1	1	92.100.	30.3		TCMP	ECHO	(pring)	reque	:5L								
1634	9819.	34155 40.40	.40.2	5	0.30.30			ICMP	Desti	nation	unrea	ichabli	e (Cor	nmunic	ation a	idmini:	strativ	ely t	Itere	a)
163	9819.	38835 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	est								
163	5 9819.	43515 40.40	.40.2	3	0.30.30	.1		ICMP	Desti	nation	unnea	ichab I (e (Cor	nmunic	ation a	admini	strativ	/ely fi	lltere	d)
163	9819.	48195 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	est								
163	3 9819.	52875 40.40	.40.2	3	0.30.30	.1		ICMP	Desti	nation	unnea	ichab]	e (Cor	nmunic	ation a	admini	strativ	/ely fi	iltere	d)
1639	9 9819.	57555 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	st								
164() 9819.	62235 40.40	.40.2	3	0.30.30	.1		ICMP	Desti	nation	unnea	ichab]	e (Cor	nmunic	ation a	admini	strativ	/ely fi	lltere	d)
1641	9819.	66915 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	st								
1642	2 9819.	68475 40.40	.40.2	3	0.30.30	.1		ICMP	Desti	nation	unnea	ichab]	e (Cor	nmunic	ation a	admini	strativ	/ely f	iltere	d)
164	3 9821.	47876 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	st								
1644	9821.	5255640.40	.40.2	3	0.30.30	.1		ICMP	Desti	nation	unnea	ichab]	e (Cor	nmunic	ation a	admini	strativ	/ely fi	iltere	d)
164	5 9821.	57236 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	st								
164	5 9821.	61916 40.40	.40.2	3	0.30.30	.1		ICMP	Desti	nation	unnea	ichab]	e (Cor	nmunic	ation a	admini	strativ	vely f	iltere	:d)
1647	7 9821.	66596 30.30	.30.1	1	92.168.	50.5		ICMP	Echo	(ping)	reque	st								
164	9821	71276.40 40	40.2	3	0 30 30	1		TCMP	Desti	nation	unnea	chab1	e (Cor	nmunic	ation a	dmini	strativ	/elv f	ltere	d) -
							_					111								
Fram	e 1: 2	4 bytes on	wire (1	92 bits)	, 24 by	tes ca	pture	ed (192	bits)											
Cisc	O HDLC								,											
Cisc	O SLAR	P																		

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.

S	SW3 1 to R1 FastEthernet2/1 Capturing from Standard input - Wireshark																				
ile	Edi	it <u>V</u> iew	Go	<u>C</u> apture	Anal	yze	Statistic:	s Te	lephony	<u>/ I</u> o	ols <u>H</u>	elp									
Ņ		e	2		8	2	8 (2, 4		\$ 💫	₹ 1] Q Q		••••	1	1 %				
Filte	er:										•	Expression	Clear	Apply							
о.		Time		Source				Destin	nation			Protocol	Info								
	56	278.4	05103	ca:01	:13:8	38:0	0:39	CDP/	VTP/	DTP/I	PAgP/	UDCDP	Device	ID: A	AA.far	rah	Port I	D: Fa	astEth	nernet	2/1
	57	279.9	96305	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	58	290.0	11523	ca:01	:13:8	88:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	59	300.0	11141	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	60	300.5	25942	ca:08	:18:7	'c:0	0:00	CDP/	VTP/I	DTP/I	PAgP/	UDCDP	Device	ID: p	c4.PC4	4 PC	rt ID:	Fast	tEther	net0/	0
	61	310.0	06965	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	62	320.0	06582	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	63	324.1	24990	192.1	68.10	0.3		20.2	20.20	.1		TCP	50977 >	ssh	[SYN]	Seq=	0 Win=4	4128	Len=() MSS=	536
	64	327.9	31396	192.10	68.10	0.3	0	20.2	20.20	.1		TCP	50977 >	ssh	[SYN]	Seq=	0 Win=4	4128	Len=0) MSS=	536
	65	330.0	06200	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	66	335.8	25010	ca:01	:13:8	38:0	0:39	CDP/	VTP/I	DTP/I	PAgP/	UDCDP	Device	ID: A	AA.far	rah	Port I	D: Fa	astEth	nernet	2/1
	67	340.0	05818	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
	68	340.7	23419	192.10	68.10	0.3		20.2	20.20	.1		TCP	38600 >	- ssh	[SYN]	Seq=	:0 Win=4	4128	Len=0) MSS=	536
	69	344.5	14226	192.10	68.10	0.3		20.2	20.20	.1		TCP	38600 >	ssh	[SYN]	Seq=	:0 Win=4	4128	Len=0) MSS=	536
	70	350.0	21035	ca:01	:13:8	38:0	0:39	ca:()1:13	:88:	00:39	LOOP	Reply								
E	ram	e 1: 60	0 bvt	es on	wire	(48	0 bit	s). (50 bv	tes	captu	red (480	bits)								
I E	the	rnet I	I. Sr	c: ca:	01:1	3:88	:00:3	9 (c	a:01:	13:8	8:00:	39). Dst	: ca:01:	13:88	:00:39) (ca	:01:13:	:88:0	0:39)		
	onf	igurat	ion T	est Pr	otoc	01 (loopb	ack)													
D	ata	(40 b)	vtes)																		
			, ,																		



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022- Available at www.ijraset.com

2) Test ping from 192.168.100.2 to 192.168.200.2 no response found

1	SW3 1 to R1 FastEthernet2/1 Capturing from Standard input - Wireshark														
<u>F</u> ile	e <u>E</u> di	it <u>V</u> iew <u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	Statistics	s Telephon	<u>y T</u> ools	<u>H</u> elp)						
		M 🛯 🕅		XR	8 0	2, 🗢 🔿	4	₽		Ð,	ର୍ ପ୍	m 👹	¥ 🍢	*	Ø
Filt	ter:							•	Expression.	Clea	r Apply				
١o.		Time	Source		_	Destination			Protocol	Info					
	141	756.60295	9 192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	142	758.63096	2 192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	143	760.00376	5 ca:01:	13:88:0	0:39	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	771.05179	1 192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	147	773.07979	5192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	148	775.10779	8192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	149	777.13580	2 192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	150	779.16380	5192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	151	780.00620	7 ca:01:	13:88:0	00:39	ca:01:13	:88:00:	39	LOOP	Reply					
	152	783.01701	2 192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	153	785.04501	6192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	154	787.07301	9192.16	8.100.2	2	192.168.	200.2		ICMP	Echo	(ping)	request			
	155 789.101023 192.168.100.2 192.168.200.2 ICMP Echo (ping) request														
Ð	Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)														
Ð	Ethe	rnet II. S	rc: ca:(01:13:8	8:00:3	9 (ca:01:	13:88:0	0:39), Dst	ca:0	1:13:8	8:00:39	(ca:01	:13:88	:00:39)
Đ	Configuration Test Protocol (loopback)														
Đ	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.

SW2 1 to R1 FastEthernet0/0 Capturing from Standard input - Wireshark										
<u>File Edit View Go Capture Analyze Statisti</u>	cs Telephon <u>y T</u> ools <u>H</u> elp									
	् 🗧 🔿 🤣 🕇 👱 🛙 🗐 🗐] 0, 0, 0, 17 🖼 🗵 🥵 % 💢								
Filter:	 Expression 	n Clear Apply								
No. Time Source	Destination Protocol	Info								
2 0.015600 Ca:01:13:88:00:00	Ca:01:13:88:00:00 LOOP	керту								
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 MS5=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 17 721202 102 100 200 2 102 102 100 2 TCB 12062 5 tolant [CVII] Con_0 Win_4120 100_0 MEC_526										
Frame 1: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits)										
# IEEE 802.3 Ethernet										
H Logical-Link Control										
🗄 Cisco Discovery Protocol										



International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538

Volume 10 Issue VI June 2022- Available at www.ijraset.com

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

SW	W2 1 to R1 FastEthernet0/0 Capturing from Standard input - Wireshark																		
ile	<u>E</u> dit <u>V</u> i	ew <u>G</u> o	Capture	<u>Anal</u>	yze	Statistics	elephon	y <u>T</u> ools	He	р									
		91 94		8 ×	2	8 Q	\$	۹۶ 🚱	₹		⊕, €	Q Q	••		¥ 🍕	* 1	g i		
ilter									•	Expression	Clear	Apply							
.	Time		Source			De	tination			Protocol	Info								
-	252 125	7.0924	3 192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 LAC	скј	Seq=1	ACK=3/	W1n=409	2 Le	n=0
- 2	253 125	7.2328	33 192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	c		
- 2	254 125	7.4356	3192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	c		
2	255 125	7.4668	33 192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 [AG	CK]	Seq=1	Ack=39	Win=409	0 Le	n=0
2	256 125	7.6384	3 192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contin	nuation	n or	non	-HTTP	traffi	с		
2	257 125	7.6540	3:192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 [AG	cK]	Seq=1	Ack=41	Win=408	8 Le	n=0
- 2	258 125	7.8568	3 192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	c		
2	259 125	7.8568	33 192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 [AG	CK]	Seq=1	Ack=43	Win=408	6 Le	n=0
2	260 125	8.0596	3 192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	с		
2	261 125	8.0752	3 192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 [AG	CK]	Seq=1	Ack=45	Win=408	4 Le	n=0
2	262 125	8.2156	3192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	с		
2	263 125	8.2468	33 192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 [AG	CK]	Seq=1	Ack=49	Win=408	0 Le	n=0
2	264 125	8.6680	3 192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	с		
2	265 125	8.8708	3 192.1	168.20	0.3	19	2.168.	100.3		HTTP	Contir	nuation	n or	non	-HTTP	traffi	c		
2	266 125	8.9020	3 192.1	168.10	0.3	19	2.168.	200.3		TCP	http >	> 12624	4 [AG	ck]	Seg=1	Ack=51	win=407	8 Le	n=0
_	167 175	0 0001	101 101 1	160 10	NO 7	10	1 1 6 0	200.2		TCD	httn .	1262	4 F.A.	cv3	Con 1	Acle 50	win 407		n 0
_					_				_				_	1	11			_	
Fr	ame 1:	373 b	ytes o	n wire	e (2	984 bits), 373	bytes	cap	tured (2	2984 bi	ts)							
TE	FF 802	3 Eth	ernet																

Logical-Link Control

E Cisco Discovery Protocol

Table (4.1) this table	explains the result showed	of the comparison between	CBAC and ZBF firewalls.
	1	1	

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











45.98



IMPACT FACTOR: 7.129







INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 🕓 (24*7 Support on Whatsapp)