ITCS 461 Computer & Communication Security  ID: 6288102 Name: Krissanapong Palakham Section: 1
<u>Lab 8 : Firewall</u>
Follow Lab 8 document (Lab8.pdf) and answer these questions:
Part I: Without Firewall
no question in this part
Part II: With Firewall
<ul> <li>Question 1: <ol> <li>Observe the traffic flowing from the Internet into your system or from your network to the Internet. Is your network connected to the Internet? N (Y/N)</li> <li>Explain why or why not: Because it has a firewall. Add some active attacks by clicking on several different options.</li> <li>Are these attacks able to get into your network? N (Y/N)</li> <li>Do you feel your system is secure? Y (Y/N)</li> <li>What's wrong with this scenario? The system cannot connect to the internet</li> </ol> </li></ul>
<ul> <li>Question 2: What is firewall rule which allows only Email traffic to go out?</li> <li>Source IP: Mail Port: 25</li> <li>Destination IP: Any Port: *</li> <li>Protocol: TCP</li> </ul>
(Create firewall rule named, "Email out", similar to DNS out, try until you get success, copy IP, Port and Protocol from Firewall1 Rule window to your answer.)

window to your answer.) copy IP, Port and Pr

<b>Question 3:</b> What is firewall rule wh	ich allows o	nly Email	traffic to d	come in ?
<ul><li> Source IP : Any</li><li> Destination IP : Mail</li></ul>	Port	: 25	<del></del> 5	
• Protocol : TCP			<u> </u>	
	_			
(Move "Email out" rule to <u>Inactive</u> ! "Email in", similar to Email out, but Email, try until you get success, copy to your answer.)	define source	ce IP as a	ny and dest	tination IP as
Question 4: What is a set of firewall and go out?	rules which	allows or	nly Email t	raffic to come in
The 1st Rule:	Dont	. 25	<b>-</b>	
<ul><li> Source IP : Mail</li><li> Destination IP : Any</li></ul>	Port	:	<u> </u>	
	Port	•		
• Protocol : <u>TCP</u>				
The 2nd Rule:  Source IP: Mail  Destination IP: Any  Protocol: TCP	Port Port	: <u>25</u> : *	5	
(Combine, "Email in" and "Email or you get success, copy IP, Port and Pranswer.)				• • •
<ul> <li>Question 5:</li> <li>Change a sequence of Email in traffic still flow? Y (Y/N)</li> <li>Why? Because of Email</li> </ul>	)			
•				•
Question 6: What is a rule which allows all inbou	and traffics?			
• The 1st Rule:				
<ul><li>Source IP : Any</li><li>Destination IP :</li></ul>		_ Port : _	*	
		_ Port : _	53	
<ul><li>Protocol : <u>UDP</u></li></ul>	<u>_</u>			
• The 2nd Rule:				
• Source IP : <u>Any</u>		_ Port : _	*	
<ul><li>Destination IP :</li></ul>	Mail	_ Port : _	25	
<ul><li>Protocol :TCP</li></ul>	_			

• [	<u> The 3rd Rule :</u>					
0	C ID	Any		_ Port :	*	_
0	D ID	•	Database		Port :	3306
o	Protocol:		_			
• [	Γhe 4th Rule:					
0	Source IP:	Any		_ Port :	*	_
o	D 1 1 TD				38287	7
0	D . 1					
• [	Γhe 5th Rule:					
0	Source IP:	Any		Port:	*	
0	Destination IP:	•	Web	Port :	80	_
	Protocol:		_	<del></del>		
	The 6th Rule:					
·	Source IP :	Any		Port :	*	_
	Destination IP:					_
	Protocol:					
			<del>_</del>			
What is	s a rule which <u>allow</u>	<u>/s</u> all <u>outbo</u>	ound traffics	?		
• [	<u> Γhe 1st Rule :</u>					
o	Source IP:	DNS		Port :	53	_
o	Destination IP:		Any	Port :	*	_
o	Protocol:	UDP	<u>-</u>			
	<u> The 2nd Rule :</u>					
0	Source IP:	Mail		_ Port :	25	_
0	Source IP : Destination IP :		Any	Port :	*	_
	Protocol:		_			
	The 3rd Rule:					
· · · · · · · · · · · · · · · · · · ·		Datab	oase		Port :	3306
0	D ' ' ID			Port :	*	
0	D 1		_			
• [	The 4th Rule :					
0		VOIP	)	Port:	38287	7
o	D ' ' ID				*	
o	D . 1			<del></del>	_	
• [	<u>Fhe 5th Rule</u> :		<del>_</del>			
<u>-</u>	C ID	Web		Port :	80	
0	TO 11 11 TTD			Port :	*	_
0	D . 1			<u> </u>		
• -	The 6th Rule:	<u> </u>	_			
0	C TD	Chat		Port ·	5222	
	Destination IP:			<del></del>	*	_

0	Protocol:_	TCP	<u>—</u>	
• What	is a rule whi	ch blocks all tr	affics?	
		Default fire	ewall rule	

## **Question 7:**

How many rules do we need? Write down all of them.

Source IP	Port	Destir	nation IP		Port		Protocol
• The 1	st Rule:						
· So	ource IP :	Any		Port :		*	_
• D	estination IP:		Web	Port:		80	_
o Pr	rotocol:	TCP					
• <u>The 2</u>	2nd Rule:						
° So	ource IP :	Databa	ase		Port:		3306
	estination IP:						
o Pr	rotocol :	TCP					
• The 3	Brd Rule:						
° So	ource IP :	VOIP		Port:		38287	1
• D	estination IP:		Any	Port:		*	
	rotocol:		·				
• The 4	th Rule:						
· So	ource IP :	Any		_ Port :		*	
	estination $\overline{\text{IP}}$ :			Port :		38287	<u>-</u> '
	rotocol:		-				

## Part III: With 2 Firewalls

## **Question 8:**

What is a set of firewall rules such that **Firewall 1** allows only **DNS**, **Chat** and **Email** to come <u>in and out</u>, **Firewall 2** allows only **Chat** and **Email** to come <u>in and out</u>.

Source IP	Port	Destination	IP	Port		Protocol
Firewall 1						
• The 1st Rule:						
<ul><li>Source IP :</li></ul>	Any		Port	:	*	
<ul> <li>Destination IP</li> </ul>	:	DNS	Port	:	53	
<ul><li>Protocol :</li></ul>	UDP	<u></u>				
• The 2nd Rule:						
• Source IP :	DNS		Port	·	53	
<ul> <li>Destination IP</li> </ul>	:	Any	Port	:	*	
<ul><li>Protocol :</li></ul>	UDP		_			

The 3rd Rule:				
<ul><li>Source IP :</li></ul>	Any		Port :	*
• Destination IP:		Chat	Port :	5222
• Protocol:	TCP	_		
The 4th Rule:				
• Source IP :	Chat		Port :	5222
• Destination IP:				
• Protocol:	TCP	_		
The 5th Rule:				
<ul><li>Source IP :</li></ul>	Any		Port :	*
• Destination IP:			Port :	25
• Protocol:	TCP	<u>_</u>		
The 6th Rule:				
• Source IP :	Mail		Port :	25
• Destination IP:				
• Protocol:	TCP	-		
all 2				
The 1st Rule:	Anv		Port :	*
The 1st Rule: Source IP:	-		Port : Port :	
The 1st Rule:  Source IP:  Destination IP:			Port : Port :	
The 1st Rule:  Source IP:  Destination IP:  Protocol:				
The 1st Rule:  Source IP:  Destination IP:  Protocol:  The 2nd Rule:	ТСР	Chat	Port :	5222
The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP:	TCP Chat	Chat _	Port : Port :	5222 5222
The 1st Rule:  Source IP:  Destination IP:  Protocol:  The 2nd Rule:	TCP Chat	Chat _	Port : Port :	5222 5222
The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP: Destination IP: Protocol:	TCP Chat	Chat _	Port : Port :	5222 5222
The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP: Destination IP: Protocol: The 3rd Rule:	TCP Chat	Chat  Any	Port : Port :	5222 5222 *
The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP: Destination IP: Protocol: The 3rd Rule:	TCP Chat TCP Any	Chat  Any	Port : Port : _ Port :	5222 * *
The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Destination IP: Protocol: The 3rd Rule: Source IP: Source IP:	TCP Chat TCP Any	Chat  Any	Port : Port : Port : Port :	5222 * *
The 1st Rule: Source IP: Destination IP: Protocol: The 2nd Rule: Source IP: Destination IP: Protocol: The 3rd Rule: Source IP: Destination IP: Destination IP:	TCP Chat TCP Any	Chat  Any	Port : Port : Port : Port :	5222 * *
The 1st Rule:  Source IP:  Destination IP:  Protocol:  The 2nd Rule:  Source IP:  Destination IP:  Protocol:  The 3rd Rule:  Destination IP:  Protocol:  The 3rd Rule:  Protocol:  Protocol:	TCP Chat TCP Any TCP	Chat  Any  Mail	Port : Port : Port : Port :	5222 *  *  25
<ul> <li>Destination IP:</li> <li>Protocol:</li> <li>The 2nd Rule:</li> <li>Source IP:</li> <li>Destination IP:</li> <li>Protocol:</li> <li>The 3rd Rule:</li> <li>Source IP:</li> <li>Destination IP:</li> <li>Protocol:</li> <li>The 4th Rule:</li> </ul>	TCP Chat TCP Any TCP Mail	Chat  Any  Mail	Port : Port : Port : Port : Port :	5222 *  *  25