## Linux® Firewalls 0-7357-0900-9

Robert L. Ziegler

Copyright@ 2000 by New Riders Publishing

Warning and Disclaimer: Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information is provided on an as-is basis. The authors and New Riders Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

Misprint	Correction		
Page 3, an ASDL line	a DSL line		
Page 6, Subnet layer	Subnet layer		
Copper wire, fiberoptic cable, microwave	Copper wire, fiberoptic cable, microwave, & radio.		
Page 11, Protocol: UDP			
Source address: 192.168.10.30			
Source port: 14000			
Destination address: 10.10.22.85			
Destination port: 14000	Destination port: 123(ntp)		
Page 11, Protocol: UDP			
Source address: 10.10.22.85			
Source port: 123	Source port: 123(ntp)		
Page 12, The combination of the client's IP address	The combination of the client's IP address, port		
and port number defines the client's socket.	number, and transport protocol defines the client's socket.		
Page 12, On the server side, the combination of host	On the server side, the combination of host IP,		
IP address and the server's famous port number	address, the server's famous port number, and		
forms the server's socket.	transport protocol, forms the server's socket.		
Page 12, Each individual connection between a	Each individual connection between a given client		
given client and server, possibly just one in a set of	and server, possibly just one in a set of simultaneous		
simultaneous connections to that server (eg., a	connections to that server (e.g., a Web server), is		
Web server), is uniquely identified by both the	uniquely identified by the source address and port		
source address and port number of the client in	number of the client in conjunction with the server's		
conjunction with the server's IP address and	IP address, assigned port number, along with the		
assigned port number.	transport protocol used by the application.		
Page 21, Physical layer	Physical layer		
Copper wire, fiberoptic cable, microwave	Copper wire, fiberoptic cable, microwave, & radio.		
Page 75, Table 3.2	Table 3.2		
Numeric Type	Type Code		
Page 88, Allowing Your DNS Lookups as a Peer-to- Peer Server	Allowing Your DNS Lookups as a Peer-to-Peer Forwarding Server		
Page 114, Table 3.17 lists the local client to remote	Table 3.17 lists the complete client/server exchange		
server connection protocol	protocol		
Page 118, ntpdate is the client program and uses a	ntpdate is the client program, and can use either		
client-to-server relationship.	client-to-server or peer-to-peer communication.		
Page 124,the important thing to remember is that	the important thing to remember is that DNS		
named must be running before the firewall script	traffic must be enabled before the hostnames are		
executes.	encountered in the script.		
Page 166, Table 4.9			
Description: Choke client query In/Out: In	Description: Choke client query In/Out: Out		

<b>Description:</b> Bastion server response <b>In/Out:</b> Out		<b>Description:</b> Bastion server response <b>In/Out:</b> In					
Page 169, Table 4.13 Choke SMTP Mail Protocol on a DMZ Client			Table 4.13 Choke Client SMTP Mail Protocol to a DMZ Server				
Page 174, Table 4.19			Table 4.19				
Remote Address	Remote Port	In/Out	Remo	te Address		Remote Port	
NEWS SERVER	119	In		KE DMZ IPADDI	2	1024 : 65535	
NEWS SERVER	119	Out		KE_DMZ_II ADDI KE_DMZ_IPADDI		1024 : 65535	
NNTP clients	1024 : 65535			S SERVER DMZ		119	
						119	
NNTP clients	1024 : 65535	In		S_SERVER_DMZ			
NEWS_FEED	119	Out		S_SERVER_DMZ		1024 : 65535	
NEWS_FEED	119	In		S_SERVER_DMZ		1024 : 65535	
Local Address		Local Port		t Local Address		cal Port	
CHOKE_DMZ_IPAD		1024 : 65535	In	NEWS_SERVE		19	
CHOKE_DMZ_IPAD		1024 : 65535	Out	NEWS_SERVE			
NEWS_SERVER_DN	MZ_IPADDR	119	Out	NNTP clients		024 : 65535	
NEWS_SERVER_DN	MZ_IPADDR	119	In	NNTP clients	1	024 : 65535	
NEWS_SERVER_DN	MZ_IPADDR	1024 : 65535	In	NEWS_FEED	11	19	
NEWS_SERVER_DN	MZ_IPADDR	1024 : 65535	Out	NEWS_FEED	11	19	
	175, Table 4.20				ole 4.20		
Description	Local Addr	ess		ription L	ocal Addres	S	
Choke client query	IPADDR			e client query C			
DMZ server response			DMZ server response CHOKE_DMZ_IPADDR				
	192, Table 4.35				ole 4.35		
Remote Port	<b>Local Port</b>		Remo	Remote Port Local Port			
WEB_PROXY_PORT	Γ 1024 : 6553	5	1024	: 65535	WEB_PROX	XY_PORT	
WEB_PROXY_POR	T 1024: 6553	5	1024	: 65535	WEB_PROX	KY_PORT	
Page 193, T	ables 4.36, 4.37,	4.38	Tables 4.36, 4.37, 4.38				
Local Address CHOR	KE DMZ IPAD	DRIPADDR	Local Address CHOKE_DMZ_IPADDR				
	195, Table 4.39		Table 4.39				
Remote Address	Remote Po	rt	Remote Address Remote Port				
ANYWHERE	80			ADDRESSES			
ANYWHERE	80			ADDRESSES			
			_	Local Address Local Port			
			ANYWHERE 80				
	MZ_ADDRESSES 1024 : 65535		ANYWHERE 80				
DMZ_ADDRESSES 1024 : 65535 Page 195, Table 4.40			Table 4.40				
Remote Address	193, 1able 4.40 <b>Remot</b>	o Dout	Dame	ote Address	Remote	Dout	
		e rort					
ANYWHERE	443		-	_ADDRESSES	1024 : 63		
ANYWHERE	443	D 4		_ADDRESSES	1024 : 63		
Local Address	Local			Address	Local Po	ort	
DMZ_ADDRESSES		65535		WHERE	443		
DMZ_ADDRESSES	1024 :	65535	ANY	WHERE	443		
						_	
Daga	227, Table 4.73			Tal	ole 4.73		
Local Address		te Address	Remo	ote Address		cal Address	

CHOKE_DMZ_IPADDR	CHOKE_LAN_ADDRESSES
CHOKE_DMZ_IPADDR	CHOKE_LAN_ADDRESSES
Page 369	22/UDP—PC Anywhere (old version)
• 22/UDP—PC Anywhere (old version)	input DENY eth0 PROTO=17
input DENY eth0 PROTO=17 10.10.22.85:14386	10.10.22.85:14386 192.168.10.30:22
192.168.10.30:2	

This errata sheet is intended to provide updated technical information. Spelling and grammar misprints are updated during the reprint process, but are not listed on this errata sheet.