

XYZ, Inc. Firebox Report

April 2002
Created by autoDOC

Firebox: MyBox



WatchGuard Firebox System - Version 4.61

Report printed on pc3 at 04/19/02 14:42:04

Table of Contents

1. Network Configuration	1
1.1 Interface List	1
1.2 Dynamic Network Address Translation	1
1.3 Drop-In Configuration	2
1.4 Additional Routes	2
1.5 DHCP Server	2
1.6 Site Info	2
2. Authentication	3
2.1 Aliases	3
2.2 Firebox Users	3
2.3 Authentication	3
3. Options	4
3.1 Default Packet Handling	4
3.2 Blocked Sites	4
3.3 Blocked Ports	4
3.4 Spam Screen	5
4. Virtual Private Networking	6
4.1 Gateways	6
4.2 Tunnels	6
4.3 Policies	6
4.4 DVCP	6
4.5 WatchGuard VPN	6
4.6 PPTP	7
5. Service Configuration	8
5.1 Any	8
5.2 AOL	8

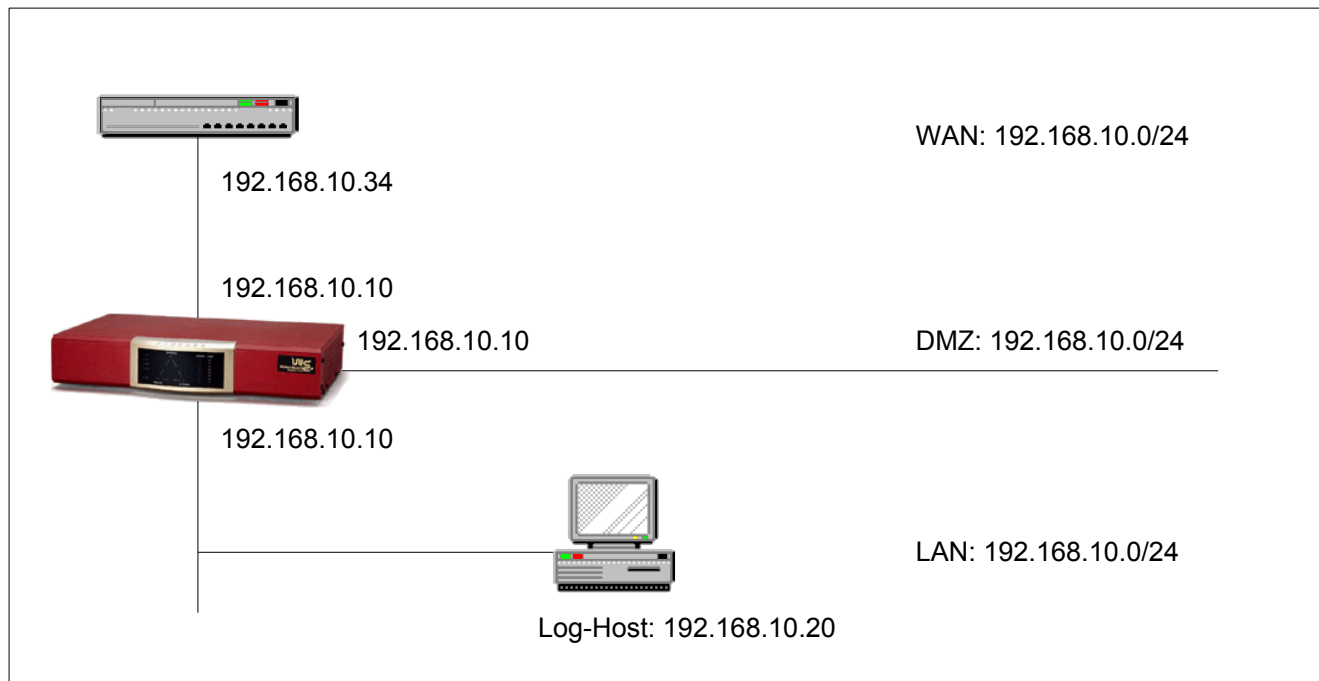
5.3 archie	9
5.4 auth	9
5.5 Citrix	10
5.6 Clarent-command	11
5.7 Clarent-gateway	11
5.8 CU-SeeMe	12
5.9 DCE-RPC	12
5.10 DHCP-Client	13
5.11 DHCP-Server	14
5.12 DNS	14
5.13 DVCPv2	15
5.14 Filtered-HTTP	15
5.15 Filtered-SMTP	16
5.16 finger	17
5.17 FTP	17
5.18 gopher	18
5.19 H323	18
5.20 HBCI	19
5.21 HTTP	20
5.22 HTTPS	21
5.23 IMAP	21
5.24 LDAP	22
5.25 LotusNotes	22
5.26 MS-SQL-Monitor	23
5.27 MS-SQL-Server	23
5.28 MyService	24
5.29 NNTP	25
5.30 NTP	25
5.31 Outgoing	26

5.32 Outgoing-TCP	26
5.33 Outgoing-UDP	27
5.34 pcANYWHERE	27
5.35 ping	28
5.36 POP2	29
5.37 POP3	29
5.38 PPTP	30
5.39 Proxied-HTTP	30
5.40 Proxy	31
5.41 RADIUS	32
5.42 RealNetworks	33
5.43 RIP	33
5.44 RTSP	34
5.45 SMB	34
5.46 SMTP	35
5.47 SNMP	36
5.48 SNMP-trap	37
5.49 Soho_Management_Gateway	38
5.50 SQL*Net	38
5.51 SQL-Server	39
5.52 ssh	39
5.53 StreamWorks	40
5.54 syslog	41
5.55 TACACS	41
5.56 TACACS+	42
5.57 telnet	42
5.58 Timbuktu	43
5.59 time	43
5.60 traceroute	44

5.61 VDOLive	44
5.62 WAIS	45
5.63 WatchGuard	46
5.64 WatchGuard-Logging	46
5.65 wg_dhcp_server	47
5.66 wg_pptp	47
5.67 wg_vpn_00	48
5.68 whois	48

1. Network Configuration

Firebox is configured in drop-in operation mode.



1.1 Interface List

Interface	Address	Network	Netmask	Default Gateway
External Interface (eth0)	192.168.10.10	192.168.10.0/24	255.255.255.0	192.168.10.34
Trusted Interface (eth1)	192.168.10.10	192.168.10.0/24	255.255.255.0	none
Optional Interface (eth2)	192.168.10.10	192.168.10.0/24	255.255.255.0	none
Secondary Interface (eth0:0)	192.168.55.60	192.168.55.56/29	255.255.255.248	none
Secondary Interface (eth1:0)	172.16.50.55	172.16.50.0/24	255.255.255.0	none
Secondary Interface (eth2:0)	192.168.200.20	192.168.200.0/26	255.255.255.192	none
External Interface (Aliases)	192.168.10.11 192.168.10.12			

1.2 Dynamic Network Address Translation

Enable dynamic NAT: yes
 Dynamic NAT entries: trusted-external
 Dynamic NAT exceptions: none
 Enable service based NAT: no
 1 to 1 NAT enabled: no

1.3 Drop-In Configuration

	external	trusted	optional
Default Network		eth1	
Related hosts	192.168.10.34	192.168.10.9 192.168.10.7	192.168.10.8

1.4 Additional Routes

Type	Device	Destination	Mask	Gateway
net	any	192.168.230.0/24	255.255.255.0	192.168.10.62
host	any	192.168.220.55	255.255.255.255	192.168.10.70

1.5 DHCP Server

		From	To
DHCP Server enabled	yes		
Subnet 00	192.168.10.0/24	192.168.10.200	192.168.10.220
Subnet 01	192.168.10.0/24	192.168.10.240	192.168.10.244

1.6 Site Info

Facility	Value
Hostname	watchguard
Domain	MyDomain.org
Timezone	Indian/Mahe
Loghost(s)	192.168.10.20
Syslog-Host	192.168.10.100
DNS server 1 (VPN)	192.168.10.150
WINS server (VPN)	192.168.10.121

2. Authentication

2.1 Aliases

Aliases	Content
dvcp_nets	194.181.55.30
MyAlias	192.168.10.50 optional trusted

2.2 Firebox Users

User	Group Membership
user01	ipsec_users Mygroup pptp_users
user02	ipsec_users Mygroup pptp_users

2.3 Authentication

Authentication Type: local

Logon Timeout	60s
Session Timeout	86400s

3. Options

3.1 Default Packet Handling

Settings

Block IP Options	yes
Block Address Space Probes	yes
Block Port Space Probes	yes
Autoblock source of packets not handled	no
Send an error message to clients whose connections are blocked	yes
Log incoming packets sent to broadcast addresses	yes
Log outgoing packets sent to broadcast addresses	yes

Logging & Notification

Direction	Dispo	Logging	Notification	Program
spoofing		warning	no	
ipoptions		warning	no	
probe	address	info	no	
probe	port	warning	no	
default	incoming	warning	no	
default	outgoing	no	no	

3.2 Blocked Sites

Settings

Block Site List	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
Exceptions	

Logging & Notification

Direction	Dispo	Logging	Notification	Program
hostile_site		info	no	

3.3 Blocked Ports

Settings

Block Port List	2049 6000 6001 6002 6003 6004 6005 8000 513 514 7100 0 1 111
-----------------	--

Logging & Notification

Direction	Dispo	Logging	Notification	Program
hostile_port		warning	no	

3.4 Spam Screen

DNS Server	192.168.100.120
Spam Mail Handling	tag
Rag added to subject	
Advanced Spam Mail Filtering	yes
RBL default list	dul.maps.vix.com rbl.maps.vix.com relays.orbs.org rss.maps.vix.com
RBL list	dul.maps.vix.com rbl.maps.vix.com relays.orbs.org
Exceptions	exception.org

4. Virtual Private Networking

4.1 Gateways

Gateway	Address	Type	Shared Secret
dvcp01	194.181.55.30	ike_dvcp	sugus
	Remote ID Local ID Phase 1 Encryption Phase 1 Authentication Negotiation Timeouts Diffie Hellmann Group Enable Perfect Forward Secrecy Enable Aggressive Mode	IP Address IP Address DES-CBC SHA1-HMAC 0 KBytes or 86400 Seconds 1 No No	
Gateway01	144.155.166.177	isakmp	sugus
	Remote ID Local ID Phase 1 Encryption Phase 1 Authentication Negotiation Timeouts Diffie Hellmann Group Enable Perfect Forward Secrecy Enable Aggressive Mode	IP Address IP Address DES-CBC SHA1-HMAC 0 KBytes or 86400 Seconds 1 No No	

4.2 Tunnels

Tunnel	Gateway	DVCP
dvcp01000	dvcp01	false
SA 00	Type ESP	Encryption 3DES-CBC
	Authentication MD5-HMAC	Key Expiration 8192 KBytes or 86400 Seconds
Tunnel01	Gateway01	false
SA 00	Type ESP	Encryption 3DES-CBC
	Authentication SHA1-HMAC	Key Expiration 8192 KBytes or 86400 Seconds

4.3 Policies

Policy	Type	Tunnel	Gateway	Dispo	Source	Destination
BO-000	inbound	Tunnel01		secure	10.10.10.0/24	192.168.10.0/24
BO-000	outbound	Tunnel01		secure	192.168.10.0/24	10.10.10.0/24
RU-000	inbound	dvcp01000	dvcp01	secure	194.181.55.30	192.168.10.0/24
RU-000	outbound	dvcp01000		secure	192.168.10.0/24	194.181.55.30

4.4 DVCP

Enable this Firebox as DVCP Client?	yes
Firebox Name	MyBox
DVCP V.2 Server	134.135.136.137
Enable debug messages for DVCP client?	yes

4.5 WatchGuard VPN

id	trusted	remote	remote networks	type
00	192.168.10.10	195.166.120.21	195.161.52.0/24	RC4-128

4.6 PPTP

Activate Remote User VPN with PPTP?	yes
Enable drop from 128-bit to 40-bit?	yes
IP Adresses used	195.191.56.22
Enable control channel protocol logging (TCP 1723)	no
Enable data channel protocol logging (IP 47)	no
Enable data channel packet logging (IP 47)	no

5. Service Configuration

5.1 Any

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
Any		

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	None	None
outgoing	allow	None	None

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.2 AOL

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
tcp	5190	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Proxy Settings

Make incoming connections read only	yes
Make outgoing connections read only	no
Deny incoming SITE command	no
Force FTP session timeout	1800s
Log incoming accounting/auditing information	no
Log outgoing accounting/auditing information	no

5.18 gopher

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
tcp	70	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.19 H323

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
tcp	389	client
h323	1720	client
tcp	1503	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.20  HBCI

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
tcp	3000	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.26 MS-SQL-Monitor

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
udp	1434	client
tcp	1434	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.27 MS-SQL-Server

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
udp	1433	client
tcp	1433	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

5.29 NNTP

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
tcp	119	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.30 NTP

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
udp	123	ignore
tcp	123	ignore

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.31  **Outgoing**

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
outgoing-udp	-1	
outgoing-tcp	-1	

Filter Settings

Direction	Dispo	FROM	TO
outgoing	allow	Any	Any

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed			
incoming	denied			
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.32   **Outgoing-TCP**

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
outgoing-tcp	ÿ	

Filter Settings

Direction	Dispo	FROM	TO
outgoing	allow	Any	Any

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed			
incoming	denied			
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.33  **Outgoing-UDP**

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
outgoing-udp	ÿ	

Filter Settings

Direction	Dispo	FROM	TO
outgoing	allow	Any	Any

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed			
incoming	denied			
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.34  **pcANYWHERE**

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
tcp	65301	ignore
udp	5632	ignore
tcp	5631	ignore
udp	22	ignore

5.38 PPTP

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
ip	47	client
tcp	1723	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.39 Proxied-HTTP

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
outgoing-proxy	-1	
HTTP	80	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

Proxy Settings

Remove client connection info	yes
Remove cookies	no
Deny submissions	no
Deny JAVA applets	yes
Deny ActiveX applets	yes
Remove unknown headers	yes
Log accounting/auditing information	yes
Idle timeout	600s
Use caching proxy server	
Allow only safe content types	yes
Safe content types	text/* image/* audio/* video/* application/x-wls
Activate Webblocker	
Auto-download the webblocker database	no
Message for blocked user	Request blocked by WebBlocker
Operational blockings	
Non-operational blockings	
Webblocker allowed exceptions	
Webblocker denied exceptions	

5.40  Proxy

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
outgoing-proxy	ÿ	

Filter Settings

Direction	Dispo	FROM	TO
outgoing	allow	Any	Any

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed			
incoming	denied			
outgoing	allowed	no	no	
outgoing	denied	yes	no	

Proxy Settings

Remove client connection info yes
 Remove cookies no
 Deny submissions no
 Deny JAVA applets yes
 Deny ActiveX applets yes
 Remove unknown headers yes
 Log accounting/auditing information yes
 Idle timeout 600s
 Use caching proxy server
 Allow only safe content types yes
 Safe content types text/* image/* audio/* video/* application/x-wls
 Activate Webblocker
 Auto-download the webblocker database no
 Message for blocked user Request blocked by WebBlocker
 Operational blockings
 Non-operational blockings
 Webblocker allowed exceptions
 Webblocker denied exceptions

5.41  **RADIUS**

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
udp	1645	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	deny	Any	Any
outgoing	allow	Any	Any

Autoblock connection attempts no

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

Proxy Settings

Incoming

Idle timeout	600s
Maximum recipients	99
Maximum size	3000KB
Allow remote message queue starting	no
Address validation; allowed characters	_-.+=%*/~!^&?
Allow 8-bit characters	yes
Allow source-routed addresses	no
Allow only safe content types	yes
Safe content types	text/* image/* audio/* video/* multipart/* message/* application/x-wls
Deny attachments based on filename patterns	*.bat *.exe *.hta *.js *.vb? *.wsf *.wsh *.shs
Deny message	[Attachment denied by WatchGuard SMTP proxy (type "%t", filename
Allowed from	* %f")]
Allowed to	*
Denied from	
Denied to	
Allow these headers	X-* Received From To cc bcc Resent-To Resent-cc Resent-bcc Resent-Message-ID Resent-Reply-To Resent-From Resent-Date Resent-Sender Message-ID In-Reply-To References Keywords Subject Comments Encrypted Date Reply-To Return-path Sender MIME-Version Content-Type Content-Language Content-Length Content-Disposition Content-Transfer-Encoding Content-ID Content-Description Content-MD5 Encoding Precedence Approved-By
Log removal of unknown headers	no tus
Log removal of unknown ESMTP extensions	no
Log accounting/auditing information	no

Outgoing

Domain name	
Substitute domain for these patterns	
Do not substitute this patterns	
Masquerade Message-ID's	no
Masquerade MIME boundaries	no
Allow these header patterns	From To cc bcc Resent-To Resent-cc Resent-bcc Resent-Message-ID Resent-Reply-To Resent-From Resent-Date Message-ID In-Reply-To References Keywords Subject Comments Encrypted Date Reply-To MIME-Version Content-Type Content-Language Content-Length Content-Disposition Content-Transfer-Encoding Content-ID Content-Description Content-MD5 Encoding Precedence Approved-By Status
Log removal of unknown headers	no
Log message-ID masquerading	no
Log MIME masquerading	no
Log domain masquerading	no
Log accounting/auditing information	no

5.47 SNMP

Service added on May 14, 2001

Properties

Protocol	Ports	Client Port
udp	161	client

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.65  **wg_dhcp_server**

Properties

Protocol	Ports	Client Port
udp	67	ignore

Filter Settings

Direction	Dispo	FROM	TO
incoming	allow	0.0.0.0 optional	255.255.255.255 firebox
outgoing	allow	0.0.0.0 trusted	255.255.255.255 firebox

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

5.66  **wg_pptp**

Properties

Protocol	Ports	Client Port
tcp	1723	client

Filter Settings

Direction	Dispo	FROM	TO
incoming	allow	Any	firebox
outgoing	allow	firebox	Any

Logging & Notification

Direction	Dispo	Logging	Notification	Program
incoming	allowed	no	no	
incoming	denied	yes	no	
outgoing	allowed	no	no	
outgoing	denied	yes	no	

