Firebox Configuration Report

Firebox: Autodoc-Unit

Model: X8000
Contact: Admin
Location: BOLL Engineering AG

Firmware Version 8.2.1
Last Config Change: Wed Jan 25 18:14:45 2006

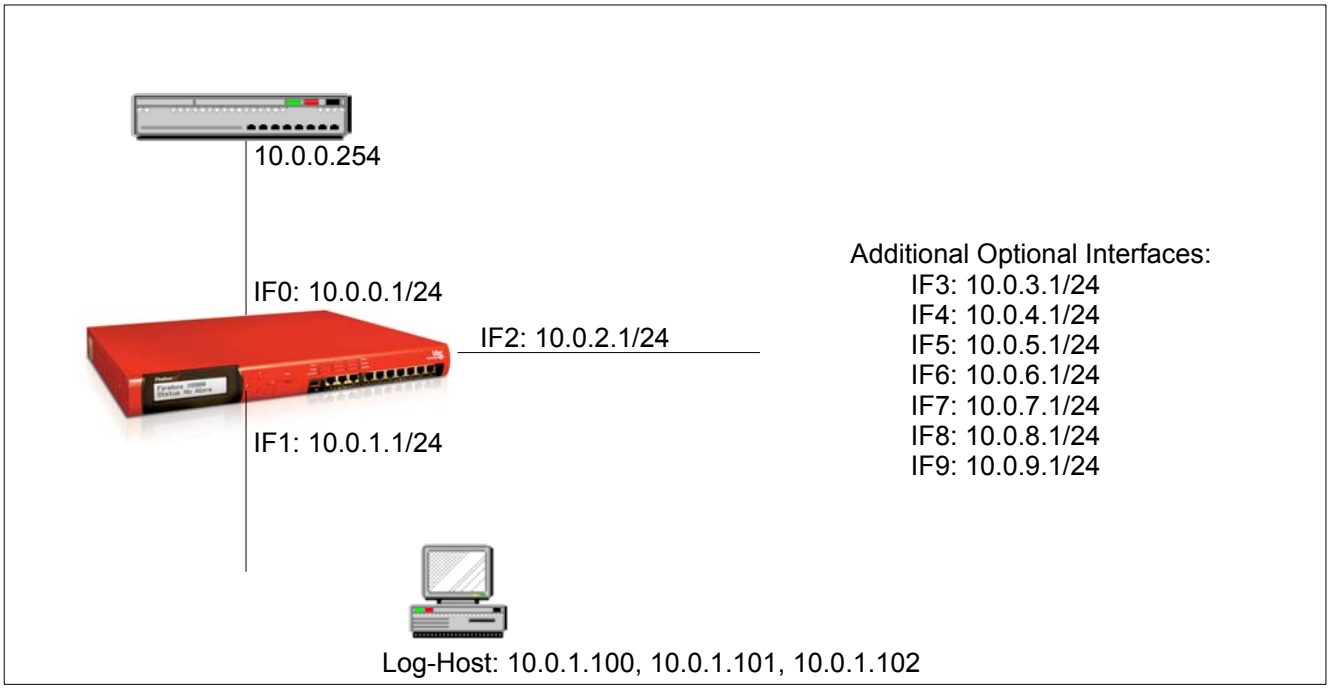
Report printed on SCSY-2 at 01/25/06 18:04:44 with autoDOC Version 6.20

Table of Contents

1. Network Configuration	**1**
1.1 Interface List	1
1.2 WINS/DNS	1
1.3 Network Address Translation	2
1.3.1 Dynamic NAT	2
2. System Configuration	**2**
2.1 Device Configuration	2
2.2 Logging	2
2.3 Authentication Servers	2
2.3.1 Firebox	2
2.4 Actions	2
2.4.1 Schedules	2
2.4.2 Proxy Actions	3
2.4.2.1 HTTP-Client	3
2.4.2.2 HTTP-Server	5
2.4.2.3 SMTP-Incoming	6
2.4.2.4 SMTP-Outgoing	9
2.4.2.5 FTP-Server	10
2.4.2.6 FTP-Client	11
2.4.2.7 DNS-Incoming	12
2.4.2.8 DNS-Outgoing	12
2.4.2.9 TCP-Proxy	13
2.5 Intrusion Preventions	13
2.5.1 Default Packet Handling	13
2.5.2 Blocked Sites	14
2.5.3 Blocked Ports	14
2.6 Global & Common Settings	14
2.7 Signature Updates	14
3. Service Configuration	**15**
3.1 Overview	15
3.2 FTP	15
3.3 Ping	16
3.4 DNS	16
3.5 WatchGuard	17
3.6 Outgoing	17
4. Virtual Private Network	**18**
4.1 Branch Office VPN	18
4.1.1 Branch Office Tunnel Policies	18
4.1.1.1 Overview	18
4.1.1.2 VPN_Tunnel-Any	18
4.1.2 Branch Office Gateways	18
4.1.3 Branch Office Tunnels	18
4.2 Mobile User VPN	19

1. Network Configuration

Firebox is configured in routed operation mode.



1.1 Interface List

No.	Type	Name	IP Address	MTU	Link-Speed	Description
0	External	External	10.0.0.1/24	1500	auto	
2	Optional	Optional-1	10.0.2.1/24	1500	auto	
3	Optional	Optional-2	10.0.3.1/24	1500	auto	
4	Optional	Optional-3	10.0.4.1/24	1500	auto	
5	Optional	Optional-4	10.0.5.1/24	1500	auto	
6	Optional	Optional-5	10.0.6.1/24	1500	auto	
7	Optional	Optional-6	10.0.7.1/24	1500	auto	
8	Optional	Optional-7	10.0.8.1/24	1500	auto	
9	Optional	Optional-8	10.0.9.1/24	1500	auto	
1	Internal	Trusted	10.0.1.1/24	1500	auto	

1.2 WINS/DNS

Parameter	Value
Domain Name	autodoc.intra
DNS Server	10.0.1.53 10.0.2.53
WINS Server	10.0.1.53

1.3 Network Address Translation

1.3.1 Dynamic NAT

From	-	To
192.168.0.0/16	-	Any-External
172.16.0.0/12	-	Any-External
10.0.0.0/8	-	Any-External

2. System Configuration

2.1 Device Configuration

Parameter	Value
System Name	Autodoc-Unit
System Location	BOLL Engineering AG
System Contact	Admin
Time Zone	(GMT+01:00) Brussels, Berlin, Bern, Rome, Stockholm, Vienna

2.2 Logging

Log Type	Status	Values
WatchGuard Log Server	enabled	Log Server: 10.0.1.100, 10.0.1.101, 10.0.1.102
Remote Syslog Server	disabled	
Firebox Internal Storage	enabled	

2.3 Authentication Servers

2.3.1 Firebox

Username	Group
muvpn1	ipsec_users
muvpn2	ipsec_users
muvpn3	ipsec_users

2.4 Actions

2.4.1 Schedules

Always On

	Sunday	0:0-24:0

MF:0700-1900

Description	Monday through Friday 7AM to 7PM	
	Monday	7:0-19:0
	Tuesday	7:0-19:0
	Wednesday	7:0-19:0
	Thursday	7:0-19:0
	Friday	7:0-19:0

Weekend

	Sunday	0:0-24:0
	Saturday	0:0-24:0

2.4.2 Proxy Actions

2.4.2.1 HTTP-Client

Default configuration for HTTP client

General

Webblocker	None	

HTTP Request

General Settings	Idle Timeout	600 sec
	Maximum URL Length	2048 bytes
	Allow range requests through unmodified	enabled (Log: disabled)
	Summary Log Message	disabled

Request Methods	Name	Rule	Action	Logging	Alarm	Disabled
	HEAD	HEAD (Exact Match)	allow			
	GET	GET (Exact Match)	allow			
	POST	POST (Exact Match)	allow			
	OPTIONS	OPTIONS (Exact Match)	allow			
	PUT	PUT (Exact Match)	allow			
	DELETE	DELETE (Exact Match)	allow			
	{fallthrough}		deny	yes		

URL Paths	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	From:*	From:* (Pattern Match)	strip/remove			
	Via:*	Via:* (Pattern Match)	strip/remove			
	Referer:*	Referer:* (Pattern Match)	strip/remove			yes
	{fallthrough}		allow			

Authorization	Name	Rule	Action	Logging	Alarm	Disabled
	Basic	Basic (Exact Match)	allow			
	Digest	Digest (Exact Match)	allow			
	NTLM	NTLM (Exact Match)	allow			
	Passport1.4	Passport1.4 (Exact Match)	allow			
	{fallthrough}		strip/remove	yes		

HTTP Response

General Settings	Idle Timeout	600 sec
	Maximum Line Length	4096 bytes
	Maximum Total Length	-

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	Accept-Ranges:*	Accept-Ranges:* (Pattern Match)	allow			
	Age:*	Age:* (Pattern Match)	allow			
	Allow:*	Allow:* (Pattern Match)	allow			
	Alternates:*	Alternates:* (Pattern Match)	allow			
	AuthData:*	AuthData:* (Pattern Match)	allow			
	Authentication-Info:*	Authentication-Info:* (Pattern Match)	allow			
	Authorization:*	Authorization:* (Pattern Match)	allow			
	Cache-Control:*	Cache-Control:* (Pattern Match)	allow			
	Connection:*	Connection:* (Pattern Match)	allow			
	Content-Base:*	Content-Base:* (Pattern Match)	allow			
	Content-Disposition:*	Content-Disposition:* (Pattern Match)	allow			
	Content-Encoding:*	Content-Encoding:* (Pattern Match)	allow			
	Content-Language:*	Content-Language:* (Pattern Match)	allow			
	Content-Length:*	Content-Length:* (Pattern Match)	allow			
	Content-Location:*	Content-Location:* (Pattern Match)	allow			
	Content-MD5:*	Content-MD5:* (Pattern Match)	allow			
	Content-Range:*	Content-Range:* (Pattern Match)	allow			
	Content-Type:*	Content-Type:* (Pattern Match)	allow			
	Content-Version:*	Content-Version:* (Pattern Match)	allow			
	Date:*	Date:* (Pattern Match)	allow			
	Derived-From:*	Derived-From:* (Pattern Match)	allow			
	ETag:*	ETag:* (Pattern Match)	allow			
	Expires:*	Expires:* (Pattern Match)	allow			
	Keep-Alive:*	Keep-Alive:* (Pattern Match)	allow			
	Last-Modified:*	Last-Modified:* (Pattern Match)	allow			
	Link:*	Link:* (Pattern Match)	allow			
	Location:*	Location:* (Pattern Match)	allow			
	MIME-Version:*	MIME-Version:* (Pattern Match)	allow			
	P3P:*	P3P:* (Pattern Match)	allow			
	Pragma:*	Pragma:* (Pattern Match)	allow			
	Proxy-Authenticate:*	Proxy-Authenticate:* (Pattern Match)	allow			
	Proxy-Connection:*	Proxy-Connection:* (Pattern Match)	allow			
	Public:*	Public:* (Pattern Match)	allow			
	Range:*	Range:* (Pattern Match)	allow			
	Retry-After:*	Retry-After:* (Pattern Match)	allow			
	Server:*	Server:* (Pattern Match)	allow			
	Set-Cookie:*	Set-Cookie:* (Pattern Match)	allow			
	Set-Cookie2:*	Set-Cookie2:* (Pattern Match)	allow			
	Trailer:*	Trailer:* (Pattern Match)	allow			
	Transfer-Encoding:*	Transfer-Encoding:* (Pattern Match)	allow			
	Upgrade:*	Upgrade:* (Pattern Match)	allow			
	URI:*	URI:* (Pattern Match)	allow			
	Vary:*	Vary:* (Pattern Match)	allow			
	Via:*	Via:* (Pattern Match)	allow			
	Warning:*	Warning:* (Pattern Match)	allow			
	WWW-Authenticate:*	WWW-Authenticate:* (Pattern Match)	allow			
	X-Dig-XMLPipe-Status:*	X-Dig-XMLPipe-Status:* (Pattern Match)	allow			
	X-Pad:*	X-Pad:* (Pattern Match)	allow			
	X-Powered-By:*	X-Powered-By:* (Pattern Match)	allow			
	{fallthrough}		strip/remove	yes		

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	text/*	text/* (Pattern Match)	allow			
	image/*	image/* (Pattern Match)	allow			
	application/pdf	application/pdf (Exact Match)	allow			
	application/x-javascript	application/x-javascript (Exact Match)	allow			
	application/x-shockwave-	application/x-shockwave-flash (Exact Match)	allow			
	application/*xml*	application/*xml* (Pattern Match)	allow			
	application/x-httpd-*	application/x-httpd-* (Pattern Match)	allow			
	httpd/*	httpd/* (Pattern Match)	allow			
	(none)		allow			yes
	{fallthrough}		deny	yes		

Cookies	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Body Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	Java bytecode	%0xcafebabe%* (Pattern Match)	deny	yes		
	ZIP archive	%0x504b0304%* (Pattern Match)	deny	yes		
	Windows EXE/DLL	%0x4d5a90000300000004000000ffff0000%* (Pattern Match)	deny	yes		
	Windows CAB archive	%0x4d53434600000000%* (Pattern Match)	deny	yes		
	{fallthrough}		allow			

Deny Message

Content-type: text/html; charset="iso-8859-1"%CRLF%%CRLF%<html>%CRLF%<body>%CRLF%<h3> %(transaction)% denied by WatchGuard HTTP proxy. </h3>%CRLF% Reason: %(reason)%
%CRLF%<hr size="1" noshade>%CRLF% Method: %(method)%
%CRLF% Host: %(url-host)%
%CRLF% Path: %(url-path)%
%CRLF%<hr size="1" noshade>%CRLF%</body>%CRLF%</html> %CRLF%

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.2 HTTP-Server

Default configuration for HTTP server

General

Webblocker	None

HTTP Request

General Settings	Idle Timeout	600 sec
	Maximum URL Length	2048 bytes
	Allow range requests through unmodified	enabled (Log: disabled)
	Summary Log Message	disabled

Request Methods	Name	Rule	Action	Logging	Alarm	Disabled
	HEAD	HEAD (Exact Match)	allow			
	GET	GET (Exact Match)	allow			
	POST	POST (Exact Match)	allow			
	OPTIONS	OPTIONS (Exact Match)	allow			yes
	PUT	PUT (Exact Match)	allow			yes
	DELETE	DELETE (Exact Match)	allow			yes
	{fallthrough}		deny	yes		

URL Paths	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Authorization	Name	Rule	Action	Logging	Alarm	Disabled
	Basic	Basic (Exact Match)	allow			
	Digest	Digest (Exact Match)	allow			
	NTLM	NTLM (Exact Match)	allow			
	Passport1.4	Passport1.4 (Exact Match)	allow			
	{fallthrough}		strip/remove	yes		

HTTP Response

General Settings	Idle Timeout	600 sec
	Maximum Line Length	-
	Maximum Total Length	-

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow	yes		

Cookies	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Body Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Deny Message

Content-type: text/html; charset="iso-8859-1"%CRLF%%CRLF%<html>%CRLF%<body>%CRLF%<h3> %(transaction)% denied by WatchGuard HTTP proxy. </h3>%CRLF% Reason: %(reason)%
%CRLF%<hr size="1" noshade>%CRLF% Method: %(method)%
%CRLF% Host: %(url-host)%
%CRLF% Path: %(url-path)%
%CRLF%<hr size="1" noshade>%CRLF%</body>%CRLF%</html> %CRLF%

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.3 SMTP-Incoming

Default configuration for incoming SMTP

General

General Settings	Idle Timeout	600 sec
	Maximum E-Mail Recipients	99
	Maximum Address Length	-
	Maximum E-Mail Size	3000 kilobytes
	Maximum E-Mail Line Length	1000 bytes
	Hide E-mail Server	by masquerading of Server-replies
	Summary Log Message	disabled

Greeting Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Non-allowed characters	[^-.0-9a-zA-Z_\[\\]] (RegExp)	deny	yes		
	Maximum length	^.{51,}$ (RegExp)	deny	yes		
	{fallthrough}		allow			

ESMTP

ESMTP Settings	Allow BDAT/CHUNKING	no
	Allow ETRN	yes
	Allow 8-Bit MIME	yes
	Allow Binary MIME	no

Authentication	Name	Rule	Action	Logging	Alarm	Disabled
	DIGEST-MD5	DIGEST-MD5 (Exact Match)	allow			
	CRAM-MD5	CRAM-MD5 (Exact Match)	allow			
	PLAIN	PLAIN (Exact Match)	allow			
	LOGIN	LOGIN (Exact Match)	allow			
	LOGIN (old-style)	=LOGIN (Exact Match)	allow			
	NTLM	NTLM (Exact Match)	allow			
	GSSAPI	GSSAPI (Exact Match)	allow			
	{fallthrough}		deny	yes		

Attachments

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	text/*	text/* (Pattern Match)	allow			
	image/*	image/* (Pattern Match)	allow			
	multipart/*	multipart/* (Pattern Match)	allow			
	message/*	message/* (Pattern Match)	allow			
	(none)		allow			
	application/x-watchguard	application/x-watchguard-locked (Exact Match)	allow			yes
	{fallthrough}		strip/remove	yes		

Filenames	Name	Rule	Action	Logging	Alarm	Disabled
	*.ade	*.ade (Pattern Match)	strip/remove	yes		
	*.asx	*.asx (Pattern Match)	strip/remove	yes		
	*.bat	*.bat (Pattern Match)	strip/remove	yes		
	*.chm	*.chm (Pattern Match)	strip/remove	yes		
	*.cmd	*.cmd (Pattern Match)	strip/remove	yes		
	*.com	*.com (Pattern Match)	strip/remove	yes		
	*.cpl	*.cpl (Pattern Match)	strip/remove	yes		
	*.crt	*.crt (Pattern Match)	strip/remove	yes		
	*.exe	*.exe (Pattern Match)	strip/remove	yes		
	*.hlp	*.hlp (Pattern Match)	strip/remove	yes		
	*.hta	*.hta (Pattern Match)	strip/remove	yes		
	*.inf	*.inf (Pattern Match)	strip/remove	yes		
	*.ins	*.ins (Pattern Match)	strip/remove	yes		
	*.isp	*.isp (Pattern Match)	strip/remove	yes		
	*.js	*.js (Pattern Match)	strip/remove	yes		
	*.jse	*.jse (Pattern Match)	strip/remove	yes		
	*.lnk	*.lnk (Pattern Match)	strip/remove	yes		
	*.mdb	*.mdb (Pattern Match)	strip/remove	yes		
	*.msi	*.msi (Pattern Match)	strip/remove	yes		
	*.msp	*.msp (Pattern Match)	strip/remove	yes		
	*.nsc	*.nsc (Pattern Match)	strip/remove	yes		
	*.pcd	*.pcd (Pattern Match)	strip/remove	yes		
	*.pif	*.pif (Pattern Match)	strip/remove	yes		
	*.reg	*.reg (Pattern Match)	strip/remove	yes		
	*.scr	*.scr (Pattern Match)	strip/remove	yes		
	*.sct	*.sct (Pattern Match)	strip/remove	yes		
	*.shs	*.shs (Pattern Match)	strip/remove	yes		
	*.vb	*.vb (Pattern Match)	strip/remove	yes		
	*.vb?	*.vb? (Pattern Match)	strip/remove	yes		
	*.wsc	*.wsc (Pattern Match)	strip/remove	yes		
	*.wsf	*.wsf (Pattern Match)	strip/remove	yes		
	*.wsh	*.wsh (Pattern Match)	strip/remove	yes		
	.{}	*.{*} (Pattern Match)	strip/remove	yes		
	*.mp3	*.mp3 (Pattern Match)	strip/remove	yes		
	*.vbs	*.vbs (Pattern Match)	strip/remove	yes		
	*.vbe	*.vbe (Pattern Match)	strip/remove	yes		
	veryfunny*	veryfunny* (Pattern Match)	strip/remove	yes		
	love-letter*	love-letter* (Pattern Match)	strip/remove	yes		
	*.avi	*.avi (Pattern Match)	strip/remove	yes		
	resume1.*	resume1.* (Pattern Match)	strip/remove	yes		
	explorer.*	explorer.* (Pattern Match)	strip/remove	yes		
	normal.*	normal.* (Pattern Match)	strip/remove	yes		
	life_stages.*	life_stages.* (Pattern Match)	strip/remove	yes		
	Life*.*	Life*.* (Pattern Match)	strip/remove	yes		
	stages*.*	stages*.* (Pattern Match)	strip/remove	yes		
	*.asf	*.asf (Pattern Match)	strip/remove	yes		
	*.ws	*.ws (Pattern Match)	strip/remove	yes		
	*.eml	*.eml (Pattern Match)	strip/remove	yes		
	*.adp	*.adp (Pattern Match)	strip/remove	yes		
	*.bas	*.bas (Pattern Match)	strip/remove	yes		
	*.jsp	*.jsp (Pattern Match)	strip/remove	yes		
	*.mde	*.mde (Pattern Match)	strip/remove	yes		
	*.msc	*.msc (Pattern Match)	strip/remove	yes		
	*.mst	*.mst (Pattern Match)	strip/remove	yes		
	*.url	*.url (Pattern Match)	strip/remove	yes		
	Mmsn_offline.htm	Mmsn_offline.htm (Pattern Match)	strip/remove	yes		
	*.pi	*.pi (Pattern Match)	strip/remove	yes		
	your_details.zip	your_details.zip (Pattern Match)	strip/remove	yes		
	your_details.zi	your_details.zi (Pattern Match)	strip/remove	yes		
	movie.zip	movie.zip (Pattern Match)	strip/remove	yes		
	screensaver.zip	screensaver.zip (Pattern Match)	strip/remove	yes		
	document.zip	document.zip (Pattern Match)	strip/remove	yes		
	application.zip	application.zip (Pattern Match)	strip/remove	yes		
	message.zip	message.zip (Pattern Match)	strip/remove	yes		
	photos.zip	photos.zip (Pattern Match)	strip/remove	yes		
	winmail.dat	winmail.dat (Pattern Match)	strip/remove	yes		
	{fallthrough}		allow			

Addresses

Mail From Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Source-routed	[!%] (RegExp)	deny	yes		
	Non-allowed characters	[^-_.+=%*/~!&@?0-9a-zA-Z] (RegExp)	deny	yes		
	*	* (Pattern Match)	allow			
	{fallthrough}		deny	yes		

Mail To Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Source-routed	*!*@* (Pattern Match)	deny	yes		
	Non-allowed characters	[^-_.+=%*/~!&@?0-9a-zA-Z] (RegExp)	deny	yes		
	*	* (Pattern Match)	allow			
	{fallthrough}		deny	yes		

Headers	Name	Rule	Action	Logging	Alarm	Disabled
	From:*	From:* (Pattern Match)	allow			
	To:*	To:* (Pattern Match)	allow			
	Cc:*	Cc:* (Pattern Match)	allow			
	Bcc:*	Bcc:* (Pattern Match)	allow			
	Resent-To:*	Resent-To:* (Pattern Match)	allow			
	Received:*	Received:* (Pattern Match)	allow			
	Resent-Cc:*	Resent-Cc:* (Pattern Match)	allow			
	Resent-Bcc:*	Resent-Bcc:* (Pattern Match)	allow			
	Resent-Message-ID:*	Resent-Message-ID:* (Pattern Match)	allow			
	Resent-Reply-To:*	Resent-Reply-To:* (Pattern Match)	allow			
	Resent-From:*	Resent-From:* (Pattern Match)	allow			
	Resent-Date:*	Resent-Date:* (Pattern Match)	allow			
	Message-ID:*	Message-ID:* (Pattern Match)	allow			
	In-Reply-To:*	In-Reply-To:* (Pattern Match)	allow			
	References:*	References:* (Pattern Match)	allow			
	Keywords:*	Keywords:* (Pattern Match)	allow			
	Subject:*	Subject:* (Pattern Match)	allow			
	Comments:*	Comments:* (Pattern Match)	allow			
	Encrypted:*	Encrypted:* (Pattern Match)	allow			
	Date:*	Date:* (Pattern Match)	allow			
	Reply-To:*	Reply-To:* (Pattern Match)	allow			
	MIME-Version:*	MIME-Version:* (Pattern Match)	allow			
	Content-Type:*	Content-Type:* (Pattern Match)	allow			
	Content-Language:*	Content-Language:* (Pattern Match)	allow			
	Content-Length:*	Content-Length:* (Pattern Match)	allow			
	Content-Disposition:*	Content-Disposition:* (Pattern Match)	allow			
	Content-Transfer-Encodi	Content-Transfer-Encoding:* (Pattern Match)	allow			
	Content-ID:*	Content-ID:* (Pattern Match)	allow			
	Content-Description:*	Content-Description:* (Pattern Match)	allow			
	Content-MD5:*	Content-MD5:* (Pattern Match)	allow			
	Encoding:*	Encoding:* (Pattern Match)	allow			
	Precedence:*	Precedence:* (Pattern Match)	allow			
	Approved-By:*	Approved-By:* (Pattern Match)	allow			
	Status:*	Status:* (Pattern Match)	allow			
	return-receipt-to:*	return-receipt-to:* (Pattern Match)	allow			
	{fallthrough}		strip/remove	yes		

AntiVirus	Name	Action	Logging	Alarm
	Virus found	strip/remove	yes	
	Attachment too large	lock	yes	
	Unable to scan	lock	yes	

Deny Message

Content-Type: text/plain; charset="iso-8859-1"%CRLF%Content-Transfer-Encoding: quoted-printable%CRLF%Content-Disposition: inline%CRLF%%CRLF%The WatchGuard Firebox which protects your network detected a message which may not be safe. %CRLF%%CRLF%Cause : %(reason)% %CRLF%Content type : %(type)% %CRLF%File name : %(filename)% %CRLF%Virus status : %(virus)% %CRLF%Action : The Firebox %(action)% %(filename)%. %CRLF%%CRLF%Your network administrator %(recovery)% this attachment.%CRLF%%CRLF%

spamBlocker	Name	Action	Logging
disabled			

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.4 SMTP-Outgoing

Default configuration for outgoing SMTP

General

General Settings	Idle Timeout	600 sec
	Maximum E-Mail Recipients	-
	Maximum Address Length	-
	Maximum E-Mail Size	3000 kilobytes
	Maximum E-Mail Line Length	1000 bytes
	Hide E-mail Server	by masquerading of Server-replies
	Summary Log Message	disabled

Greeting Rules	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

ESMTP

ESMTP Settings	Allow BDAT/CHUNKING	no
	Allow ETRN	yes
	Allow 8-Bit MIME	yes
	Allow Binary MIME	no

Authentication	Name	Rule	Action	Logging	Alarm	Disabled
	DIGEST-MD5	DIGEST-MD5 (Exact Match)	allow			
	CRAM-MD5	CRAM-MD5 (Exact Match)	allow			
	PLAIN	PLAIN (Exact Match)	allow			
	LOGIN	LOGIN (Exact Match)	allow			
	LOGIN (old-style)	=LOGIN (Exact Match)	allow			
	NTLM	NTLM (Exact Match)	allow			
	GSSAPI	GSSAPI (Exact Match)	allow			
	{fallthrough}		deny	yes		

Attachments

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Filenames	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Addresses

Mail From Rules	Name	Rule	Action	Logging	Alarm	Disabled
	*	* (Pattern Match)	allow			
	{fallthrough}		deny	yes		

Mail To Rules	Name	Rule	Action	Logging	Alarm	Disabled
	*	* (Pattern Match)	allow			
	{fallthrough}		deny	yes		

Headers	Name	Rule	Action	Logging	Alarm	Disabled
	From:*	From:* (Pattern Match)	allow			
	To:*	To:* (Pattern Match)	allow			
	Cc:*	Cc:* (Pattern Match)	allow			
	Bcc:*	Bcc:* (Pattern Match)	allow			
	Resent-To:*	Resent-To:* (Pattern Match)	allow			
	Resent-Cc:*	Resent-Cc:* (Pattern Match)	allow			
	Resent-Bcc:*	Resent-Bcc:* (Pattern Match)	allow			
	Resent-Message-ID:*	Resent-Message-ID:* (Pattern Match)	allow			
	Resent-Reply-To:*	Resent-Reply-To:* (Pattern Match)	allow			
	Resent-From:*	Resent-From:* (Pattern Match)	allow			
	Resent-Date:*	Resent-Date:* (Pattern Match)	allow			
	Message-ID:*	Message-ID:* (Pattern Match)	allow			
	In-Reply-To:*	In-Reply-To:* (Pattern Match)	allow			
	References:*	References:* (Pattern Match)	allow			
	Keywords:*	Keywords:* (Pattern Match)	allow			
	Subject:*	Subject:* (Pattern Match)	allow			
	Comments:*	Comments:* (Pattern Match)	allow			
	Encrypted:*	Encrypted:* (Pattern Match)	allow			
	Date:*	Date:* (Pattern Match)	allow			
	Reply-To:*	Reply-To:* (Pattern Match)	allow			
	MIME-Version:*	MIME-Version:* (Pattern Match)	allow			
	Content-Type:*	Content-Type:* (Pattern Match)	allow			
	Content-Language:*	Content-Language:* (Pattern Match)	allow			
	Content-Length:*	Content-Length:* (Pattern Match)	allow			
	Content-Disposition:*	Content-Disposition:* (Pattern Match)	allow			
	Content-Transfer-Encodir	Content-Transfer-Encoding:* (Pattern Match)	allow			
	Content-ID:*	Content-ID:* (Pattern Match)	allow			
	Content-Description:*	Content-Description:* (Pattern Match)	allow			
	Content-MD5:*	Content-MD5:* (Pattern Match)	allow			
	Encoding:*	Encoding:* (Pattern Match)	allow			
	Precedence:*	Precedence:* (Pattern Match)	allow			
	Approved-By:*	Approved-By:* (Pattern Match)	allow			
	Status:*	Status:* (Pattern Match)	allow			
	return-receipt-to:*	return-receipt-to:* (Pattern Match)	allow			
	{fallthrough}		strip/remove	yes		

AntiVirus	Name	Action	Logging	Alarm
	Virus found	strip/remove	yes	
	Attachment too large	lock	yes	
	Unable to scan	lock	yes	

Deny Message

Content-Type: text/plain; charset="iso-8859-1"%CRLF%Content-Transfer-Encoding: quoted-printable%CRLF%Content-Disposition: inline%CRLF%%CRLF%The WatchGuard Firebox which protects your network detected a message which may not be safe. %CRLF%%CRLF%Cause : %(reason)% %CRLF%Content type : %(type)% %CRLF%File name : %(filename)% %CRLF%Virus status : %(virus)% %CRLF%Action : The Firebox %(action)% %(filename)%. %CRLF%%CRLF%Your network administrator %(recovery)% this attachment.%CRLF%%CRLF%

spamBlocker	Name	Action	Logging
disabled			

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.5 FTP-Server

Default configuration for FTP server

General Settings

Maximum Username Length	64 bytes
Maximum Password Length	32 bytes
Maximum Filename Length	1024 bytes
Maximum Command Line Length	1030 bytes
Summary Log Message	disabled

Commands	Name	Rule	Action	Logging	Alarm	Disabled
	ABOR*	ABOR* (Pattern Match)	allow			
	APPE *	APPE * (Pattern Match)	allow			
	CDUP*	CDUP* (Pattern Match)	allow			
	CWD *	CWD * (Pattern Match)	allow			
	DELE *	DELE * (Pattern Match)	allow			
	EPRT *	EPRT * (Pattern Match)	allow			yes
	EPSV*	EPSV* (Pattern Match)	allow			yes
	HELP*	HELP* (Pattern Match)	allow			
	LIST*	LIST* (Pattern Match)	allow			
	MKD *	MKD * (Pattern Match)	allow			
	NLST*	NLST* (Pattern Match)	allow			
	NOOP*	NOOP* (Pattern Match)	allow			
	PASS *	PASS * (Pattern Match)	allow			
	PASV*	PASV* (Pattern Match)	allow			
	PORT *	PORT * (Pattern Match)	allow			
	PWD*	PWD* (Pattern Match)	allow			
	QUIT*	QUIT* (Pattern Match)	allow			
	REST *	REST * (Pattern Match)	allow			
	RETR *	RETR * (Pattern Match)	allow			
	RMD *	RMD * (Pattern Match)	allow			
	RNFR *	RNFR * (Pattern Match)	allow			
	RNTO *	RNTO * (Pattern Match)	allow			
	STAT*	STAT* (Pattern Match)	allow			
	STOR *	STOR * (Pattern Match)	allow			
	STOU*	STOU* (Pattern Match)	allow			
	SYST*	SYST* (Pattern Match)	allow			
	TYPE *	TYPE * (Pattern Match)	allow			
	USER *	USER * (Pattern Match)	allow			
	XCUP*	XCUP* (Pattern Match)	allow			
	XCWD *	XCWD * (Pattern Match)	allow			
	XMKD *	XMKD * (Pattern Match)	allow			
	XRMD *	XRMD * (Pattern Match)	allow			
	{fallthrough}		deny	yes		

Download	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Upload	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		deny	yes		

Alarm Configuration	**Parameter**
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.6 FTP-Client

Default configuration for FTP client

General Settings

Maximum Username Length	64 bytes
Maximum Password Length	32 bytes
Maximum Filename Length	1024 bytes
Maximum Command Line Length	1030 bytes
Summary Log Message	disabled

Commands	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

Download	Name	Rule	Action	Logging	Alarm	Disabled
	*.cab	*.cab (Pattern Match)	deny	yes		
	*.com	*.com (Pattern Match)	deny	yes		
	*.dll	*.dll (Pattern Match)	deny	yes		
	*.exe	*.exe (Pattern Match)	deny	yes		
	*.zip	*.zip (Pattern Match)	deny	yes		
	{fallthrough}		allow			

Upload	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow	yes		

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.7 DNS-Incoming

Default configuration for incoming DNS

General	Action	Alarm	Log
Not of class internet	deny		yes
Badly formatted query	deny		yes
Summary Log message	disabled		

OPCodes	Name	Rule	Action	Logging	Alarm	Disabled
	Query	Value = 0	allow			
	IQuery	Value = 1	deny	yes		
	Status	Value = 2	deny	yes		
	Notify	Value = 4	deny	yes		
	Update	Value = 5	deny	yes		
	{fallthrough}		deny	yes		

Query Types	Name	Rule	Action	Logging	Alarm	Disabled
	A record	Value = 1	allow			
	NS record	Value = 2	allow			
	CNAME record	Value = 5	allow			
	SOA record	Value = 6	allow			
	PTR record	Value = 12	allow			
	MX record	Value = 15	allow			
	TXT record	Value = 16	deny	yes		
	AAAA IPv6 record	Value = 28	allow			
	SRV record	Value = 33	deny	yes		
	IXFR Incremental zone transfer	Value = 251	deny	yes		
	AXFR Full zone transfer	Value = 252	deny	yes		
	ANY record	Value = 255	allow			
	{fallthrough}		deny	yes		

Query Names	Name	Rule	Action	Logging	Alarm	Disabled
	mydomain.com	mydomain.com (Pattern Match)	allow			yes
	*	* (Pattern Match)	allow			
	{fallthrough}		deny	yes		

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.8 DNS-Outgoing

Default configuration for outgoing DNS

General	Action	Alarm	Log
Not of class internet	deny		yes
Badly formatted query	deny		yes
Summary Log message	disabled		

OPCodes	Name	Rule	Action	Logging	Alarm	Disabled
	Query	Value = 0	allow			
	IQuery	Value = 1	deny	yes		
	Status	Value = 2	deny	yes		
	Notify	Value = 4	allow			
	Update	Value = 5	allow			
	{fallthrough}		deny	yes		

Query Types	Name	Rule	Action	Logging	Alarm	Disabled
	A record	Value = 1	allow			
	NS record	Value = 2	allow			
	CNAME record	Value = 5	allow			
	SOA record	Value = 6	allow			
	PTR record	Value = 12	allow			
	MX record	Value = 15	allow			
	TXT record	Value = 16	allow			
	AAAA IPv6 record	Value = 28	allow			
	SRV record	Value = 33	allow			
	IXFR Incremental zone transfer	Value = 251	allow			
	AXFR Full zone transfer	Value = 252	allow			
	ANY record	Value = 255	allow			
	{fallthrough}		deny	yes		

Query Names	Name	Rule	Action	Logging	Alarm	Disabled
	doubleclick.	*doubleclick.* (Pattern Match)	deny			yes
	messenger.yahoo.com	messenger.yahoo.com (Pattern Match)	deny			yes
	{fallthrough}		allow			

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send SNMP notification	disabled

2.4.2.9 TCP-Proxy

Default configuration for TCP Proxy

General

HTTP Proxy	HTTP-Client
Summary Log message	disabled

2.5 Intrusion Preventions

2.5.1 Default Packet Handling

Dangerous Activities	Settings	Logging
Drop Spoofing Attacks	enabled	Log
Drop IP Source Route	enabled - Threshold: 1000	Log
Block Port Space Probes	enabled - Threshold: 10 dest Ports/src IP	Log
Block Address Space Probes	enabled - Threshold: 10 dest IP/src IP	Log
Drop IPSec Flood Attack	enabled - Threshold: 1500 packets/sec	Log
Drop IKE Flood Attack	enabled - Threshold: 1000 packets/sec	Log
Drop ICMP Flood Attack	enabled - Threshold: 1000 packets/sec	Log
Drop SYN Flood Attack	enabled - Threshold: 5000 packets/sec	Log
Drop UDP Flood Attack	enabled - Threshold: 1000 packets/sec	Log

Unhandled Packets	Settings
Auto-block source of packets not handled	disabled
Send an error message to clients whose connections are disabled	disabled
Log Unhandled Internal packets	enabled
Log Unhandled External packets	enabled

DDOS Prevention	Settings	Logging
Per Server Quota	enabled - Threshold: 100 connections/sec	
Per Client Quota	enabled - Threshold: 100 connections/sec	

2.5.2 Blocked Sites

Antispyware Blocklist

Block Spyware Sites	disabled

Logging & Notification:

Duration for Auto-Blocked Sites: 20 Minutes

2.5.3 Blocked Ports

Blocked Ports List

List	1, 111, 2049, 513, 514, 6000, 6001, 6002, 6003, 6004, 6005, 7100, 8000
Auto-block sites that try to use blocked	disabled
Logging	enabled
Notification	

2.6 Global & Common Settings

Common Settings

Global Settings

Ignore DF for IPSec	disabled
IPSec Pass-through	disabled
Fragmentation Req (PMTU)	enabled
Time Exceeded	enabled
Network Unreachable	enabled
Host Unreachable	enabled
Port Unreachable	enabled
Protocol Unreachable	enabled
TCP SYN Checking	enabled
TCP MSS Adjustment	Auto Adjustment

2.7 Signature Updates

IPS Signature

Signature Update Server	https://services.watchguard.com/ipsservice/
Automatic Update	disabled
Exceptions	Signature ID:

AntiVirus Updates

Update Server	https://services.watchguard.com/avservice/
Automatic Update	disabled
Max file size	1000 kbytes
Uncompress archives	disabled

3. Service Configuration

3.1 Overview

Order	Action	Name	Log	Alarm	From	To
1	Allow/Proxy	FTP	No	No	Any-Trusted Any-Optional	Any-External
2	Allow	Ping	No	No	Any-Trusted Any-Optional	Any
3	Allow/Proxy	DNS	No	No	Any-Trusted Any-Optional	Any-External
4	Allow	WatchGuard	No	No	Any-Trusted Any-Optional	Firebox
5	Allow/Proxy	Outgoing	No	No	Any-Trusted Any-Optional	Any-External

3.2 FTP

Policy added on Wed Jan 25 17:58:07 CET 2006.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
FTP-proxy (Proxy: FTP-Client)	TCP	21	

Policy

Disposition	From	To	Logging
Allow/Proxy	Any-Trusted Any-Optional	Any-External	

Advanced

Function		
Schedule	Always On	
NAT Rules	Use 1-to-1-NAT	Use global table
	Use Dynamic NAT	Use global table
ICMP Error Handling	Use global setting	

3.3  Ping

Policy added on Wed Jan 25 17:58:07 CET 2006.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Ping	ICMP	ICMP-Type: 8 - ICMP-Code 255	

Policy

Disposition	From	To	Logging
Allow	Any-Trusted Any-Optional	Any	

Advanced

Function		
Schedule	Always On	
NAT Rules	Use 1-to-1-NAT	Use global table
	Use Dynamic NAT	Use global table
ICMP Error Handling	Use global setting	

3.4 DNS

Policy added on Wed Jan 25 17:58:07 CET 2006.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
DNS-proxy (Proxy: DNS-Outgoing)	TCP	53	
	UDP	53	

Policy

Disposition	From	To	Logging
Allow/Proxy	Any-Trusted Any-Optional	Any-External	

Advanced

Function		
Schedule	Always On	
NAT Rules	Use 1-to-1-NAT	Use global table
	Use Dynamic NAT	Use global table
ICMP Error Handling	Use global setting	

3.5 WatchGuard

Policy added on Wed Jan 25 17:58:07 CET 2006.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
WG-Firebox-Mgmt	TCP	4103	
	TCP	4105	
	TCP	4117	
	TCP	4118	

Policy

Disposition	From	To	Logging
Allow	Any-Trusted Any-Optional	Firebox	

Advanced

Function		
Schedule	Always On	
NAT Rules	Use 1-to-1-NAT	Use global table
	Use Dynamic NAT	Use global table
ICMP Error Handling	Use global setting	

3.6 Outgoing

Policy added on Wed Jan 25 17:58:07 CET 2006.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
TCP-proxy (Proxy: TCP-Proxy)	TCP	0	

Policy

Disposition	From	To	Logging
Allow/Proxy	Any-Trusted Any-Optional	Any-External	

Advanced

Function		
Schedule	Always On	
NAT Rules	Use 1-to-1-NAT	Use global table
	Use Dynamic NAT	Use global table
ICMP Error Handling	Use global setting	

4. Virtual Private Network

4.1 Branch Office VPN

4.1.1 Branch Office Tunnel Policies

4.1.1.1 Overview

Order	Action	Name	Service	Log	Alarm	Tunnel	Gateway
1	Allow	VPN_Tunnel-Any	Any	No	No	VPN_Tunnel	10.20.20.20

4.1.1.2  VPN_Tunnel-Any

Policy added on Wed Jan 25 18:12:09 CET 2006.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Any	Any		

Policy

Disposition	Addresses		Logging
Allowed	10.0.5.0/24	<==> 10.20.5.0/24	

Advanced

Function	
Schedule	Always On
ICMP Error Handling	Use global setting

4.1.2 Branch Office Gateways

Gateway	Gateway IP	Remote ID	Local ID
RemoteGateway	IP Address: 10.20.20.20	IP address: 10.20.20.20	IP address: 10.0.0.1

Credential Method	Pre-Shared Key	0987654321
Phase 1	Authentication/Encryption	MD5/DES
	Mode	Main
	Key Group	Diffie-Hellman Group 2
	SA Life	8 Hour
	NAT Traversal	Keep-alive interval: 20 seconds; Source Port 4500; Dest. Port: 4500
	IKE Keep Alive	Message interval: 30 seconds; Max failures: 5

4.1.3 Branch Office Tunnels

Tunnelname	Gateway	Addresses	
VPN_Tunnel	RemoteGateway	10.0.5.0/24	<==> 10.20.5.0/24

Phase 2 Proposal	ESP-AES-SHA1 (ESP with SHA-1 - AES (256-bit), Key Expiration: 8 Hour - 128000 KBytes), PFS with DH Group 1
Advanced	Use Any for Service, Use Local Remote Pairs for Address

4.2 Mobile User VPN

Advanced Settings

Security Policy in the MUVPN is read-write
Virtual Adapter of the Secure VPN Client is set to: Required