Firebox Configuration Report

This is an example documentation made with AUTODOC.
For more information please visit www.autodoc.com

Firebox: Autodoc

Model: M4600
Firmware Version 11.12.2

Location: Data Center 1
Contact: Support

Last Config Change: Wed May 24 09:10:01 2017

Report printed on MP at 05/24/17 09:13:47 with autoDOC Version 10.0

Table of Contents

1. System Configuration

Firebox is configured in routed operation mode.
Firebox is configured in FireCluster mode.

1.1 Device Configuration

Parameter	Value
System Name	Autodoc
System Location	Data Center 1
System Contact	Support
Time Zone	(GMT+01:00) Brussels, Berlin, Bern, Rome, Stockholm, Vienna
Automatic Feature Key Sync	enabled
Notification on feature key expiry	enabled - Email (every 15min / 10times)

1.2 Self-defined Aliases

Name	Member	Description
DNS-Server	10.0.4.53	
Email-Server	10.0.4.25	

1.3 Logging

Log Type	Status	Values
WatchGuard Log Server	enabled	10.0.4.200, 10.0.4.210
Remote Syslog Server	disabled	
Firebox Internal Storage	enabled	
Log configuration changes	enabled	

Diagnostic Log	Level
Authentication	Information
FireCluster	
Cluster Management	Error
Cluster Operation	Error
Cluster Event Monitoring	Error
Cluster Transport	Error
Firewall	Error
Management	Error
Networking	
DHCP Client	Error
DHCP Server	Error
PPP	Error
PPPoE	Warning
Dynamic Routing	Error
IPv6 Router Advertisements	Error
GWC	Error
Proxy	
Connection Framework	Error
Session manager	Error
DNS	Error
FTP	Error
H323	Error
HTTP	Error
HTTPS	Error
POP3	Error
SMTP	Error
SIP	Error
TCP-UDP	Error
Security Subscriptions	
Gateway Antivirus	Error
spamBlocker	Error
WebBlocker	Error
Reputation Enabled Defense	Error
VPN	
IKE	Information
PPTP	Error
SSL	Error
L2TP	Error

Logging for traffic sent from this device: enabled
IKE packet tracing to Firebox internal storage: enabled

1.4 Authentication

1.4.1 Firebox User

Case-sensitivity for Firebox-DB user names: disabled

Username	Group	Session Timeout	Idle Timeout
ipsec	IPSEC-Users	8 hours	30 minutes
sslvpn	SSLVPN-Users	8 hours	30 minutes

1.4.2 Authentication Servers

1.4.2.1 Active Directory

demo.local	IP:Port	Search Base	Group String
	10.0.4.8:636	dc=demo,dc=local	memberOf
	Timeout	10 sec	
	Dead Time	10 minutes	
	Login Attribute		
	DN of Searching User		
	LDAPS	disabled	

1.4.3 Authorized User/Groups

Name	Type	Auth Server	Description
Guest_Access-Hotspot-Users	Group	Any	
IPSEC-Users	Group	Firebox-DB	
SSLVPN-Users	Group	Any	
ipsec	User	Firebox-DB	
sslvpn	User	Firebox-DB	
sslvpn_group_demo	Group	demo.local	
surf_users	Group	demo.local	

1.4.4 Authentication Settings

Firewall Authentication

Session Timeout	never time out
Idle Timeout	2 hours
Multiple concurrent logins	Allow unlimited concurrent firewall authentication logins from the same accout
Auto redirect user to authentication page	disabled
Default authentication server	Firebox-DB
Send a redirect after authentication	disabled
Management Session Timeout	10 hours
Management Idle Timeout	15 minutes

Single Sign-On

Single Sign-On (SSO) with Active Directory	enabled
SSO Agent IP address	10.0.4.8
Cache data for	600 seconds

1.5 Actions

1.5.1 Traffic Management

Type	All Policy
Maximum Bandwidth	1 Kbps
Guaranteed Bandwidth	0 Kbps

1.5.2 Proxy Actions

1.5.2.1 DNS-Outgoing

Default configuration for outgoing DNS

General	Action	Alarm	Log
Not of class internet	deny		yes
Badly formatted query	deny		yes
Logging for reports	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 notification	disabled

1.5.2.2 HTTP-Client.Standard

WatchGuard recommended standard configuration for HTTP-Client with logging enabled

HTTP Request

General Settings	Idle Timeout	10 min
	Maximum URL length	4096 bytes
	Allow range requests through unmodified	enabled (Log: enabled)
	Enforce Safe Search	disabled
	Enable YouTube for Schools	disabled
	Logging for reports	enabled

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			
	COPY	COPY (Exact Match)	allow			
	LOCK	LOCK (Exact Match)	allow			
	MKCOL	MKCOL (Exact Match)	allow			
	MOVE	MOVE (Exact Match)	allow			
	PROPFIND	PROPFIND (Exact Match)	allow			
	PROPPATCH	PROPPATCH (Exact Match)	allow			
	UNLOCK	UNLOCK (Exact Match)	allow			
	BCOPY	BCOPY (Exact Match)	allow			
	BDELETE	BDELETE (Exact Match)	allow			
	BMOVE	BMOVE (Exact Match)	allow			
	BPROPFIND	BPROPFIND (Exact Match)	allow			
	BPROPPATCH	BPROPPATCH (Exact Match)	allow			
	NOTIFY	NOTIFY (Exact Match)	allow			
	POLL	POLL (Exact Match)	allow			
	SEARCH	SEARCH (Exact Match)	allow			
	SUBSCRIBE	SUBSCRIBE (Exact Match)	allow			
	UNSUBSCRIBE	UNSUBSCRIBE (Exact Match)	allow			
	CCM_POST	CCM_POST (Exact Match)	allow			
	MKACTIVITY	MKACTIVITY (Exact Match)	allow			
	CHECKOUT	CHECKOUT (Exact Match)	allow			
	MERGE	MERGE (Exact Match)	allow			
	REPORT	REPORT (Exact Match)	allow			
	CHECKIN	CHECKIN (Exact Match)	allow			
	UNCHECKOUT	UNCHECKOUT (Exact Match)	allow			
	UPDATE	UPDATE (Exact Match)	allow			
	LABEL	LABEL (Exact Match)	allow			
	VERSION-CONTROL	VERSION-CONTROL (Exact Match)	allow			
	BASELINE_CONTROL	BASELINE_CONTROL (Exact Match)	allow			
	MKWORKSPACE	MKWORKSPACE (Exact Match)	allow			
	{fallthrough}		allow	yes		

(webDAV plus extension is enabled)

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

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	From:*	From:* (Pattern Match)	allow			yes
	Via:*	Via:* (Pattern Match)	allow			yes
	Referer:*	Referer:* (Pattern Match)	allow			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			

HTTP Response

General Settings	Idle Timeout	10 minutes
	Maximum line length	4096 bytes
	Maximum total length	-

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

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	text/*	text/* (Pattern Match)	allow			
	image/*	image/* (Pattern Match)	allow			
	audio/*	audio/* (Pattern Match)	allow			
	application/pdf	application/pdf (Exact Match)	allow			
	application/x-javascript	application/x-javascript (Exact Match)	allow			
	application/x-shockwave-flash	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			
	application/x-rtsp-tunnelled	application/x-rtsp-tunnelled (Pattern Match)	allow			
	application/*	application/* (Pattern Match)	allow			
	(none)		allow			yes
	{fallthrough}		allow	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		yes
	ZIP archive	%0x504b0304%* (Pattern Match)	deny	yes		yes
	Windows EXE/DLL	%0x4d5a%* (Pattern Match)	deny	yes		
	Windows CAB archive	%0x4d53434600000000%* (Pattern Match)	deny	yes		yes
	{fallthrough}		allow			

Exceptions

*.windowsupdate.com
*.microsoft.com
*.windows.com
*.mojonetworks.com
*.cloudwifi.com
redirector.online.spectraguard.net
*.airtightnetworks.com

Deny Message

Content-type: text/html; charset="utf-8"%CRLF%%CRLF%<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">%CRLF%<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">%CRLF% <head>%CRLF% <title>%(transaction)% denied by WatchGuard HTTP Proxy</title> %CRLF% <style type="text/css">%CRLF% body {%CRLF% font-family: Arial, Helvetica, Verdana, Sans-Serif;%CRLF% font-size: small; %CRLF% font-weight: normal; %CRLF% color: #000000;%CRLF% }%CRLF% div { %CRLF% margin-left: auto; %CRLF% margin-right: auto; %CRLF% text-align: center;%CRLF% }%CRLF% .box { %CRLF% width: 600px;%CRLF% background-color: #F2F2F2; %CRLF% border-left: solid 1px #C2C2C2; %CRLF% border-right: solid 1px #C2C2C2; %CRLF% vertical-align: middle;%CRLF% padding: 20px 10px 20px 10px;%CRLF% }%CRLF% p {%CRLF% text-align: left;%CRLF% }%CRLF% .red {%CRLF% font-weight: bold;%CRLF% color: Red;%CRLF% text-align: center;%CRLF% }%CRLF% .band { %CRLF% height: 20px;%CRLF% color: White;%CRLF% background: #333333;%CRLF% width: 600px;%CRLF% border-left: solid 1px #333333;%CRLF% border-right: solid 1px #333333;%CRLF% padding: 3px 10px 0px 10px;%CRLF% }%CRLF% div#wrap {%CRLF% margin-top: 50px;%CRLF% }%CRLF% </style>%CRLF% </head>%CRLF% <body> %CRLF% %CRLF% %CRLF% %CRLF% %(transaction)% denied by WatchGuard HTTP Proxy. %CRLF% Reason: %(reason)% %CRLF% Please contact your administrator for assistance. %CRLF% More Details: %CRLF% Method: %(method)% %CRLF% Host: %(url-host)% %CRLF% Path: %(url-path)% %CRLF% %CRLF% WatchGuard Technologies, Inc. %CRLF% %CRLF% </body>%CRLF%</html>

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

1.5.2.3 DNS-Incoming.DNS_Server

Default configuration for incoming DNS

General	Action	Alarm	Log
Not of class internet	deny		yes
Badly formatted query	deny		yes
Logging for reports	enabled		

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
	demo.local	*.demo.local (Pattern Match)	allow	yes		
	{fallthrough}		deny	yes		

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

1.5.2.4 DNS-Outgoing.DNS-Server

Default configuration for outgoing DNS

General	Action	Alarm	Log
Not of class internet	deny		yes
Badly formatted query	deny		yes
Logging for reports	enabled		

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 notification	disabled

1.5.2.5 FTP-Client.Standard.Outgoing

WatchGuard recommended standard configuration for FTP-Client with logging enabled

General Settings		Auto-block
	Maximum username length	64 bytes
	Maximum password length	32 bytes
	Maximum filename length	1024 bytes
	Maximum command line length	1030 bytes
	Maximum number of failed logins per connection	6
	Logging for reports	enabled

Commands	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

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

Upload	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		AV scan	yes		

AntiVirus	Name	Action	Logging	Alarm
	When a virus is detected	drop	yes	
	When a scan error occurs	drop	yes	
	Limit scanning	1024 kilobyte(s)		

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.2.6 HTTP-Client.Standard.Outgoing

WatchGuard recommended standard configuration for HTTP-Client with logging enabled

HTTP Request		
General Settings	Idle Timeout	10 min
	Maximum URL length	4096 bytes
	Allow range requests through unmodified	enabled (Log: enabled)
	Enforce Safe Search	disabled
	Enable YouTube for Schools	disabled
	Logging for reports	enabled

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			
	COPY	COPY (Exact Match)	allow			
	LOCK	LOCK (Exact Match)	allow			
	MKCOL	MKCOL (Exact Match)	allow			
	MOVE	MOVE (Exact Match)	allow			
	PROPFIND	PROPFIND (Exact Match)	allow			
	PROPPATCH	PROPPATCH (Exact Match)	allow			
	UNLOCK	UNLOCK (Exact Match)	allow			
	BCOPY	BCOPY (Exact Match)	allow			
	BDELETE	BDELETE (Exact Match)	allow			
	BMOVE	BMOVE (Exact Match)	allow			
	BPROPFIND	BPROPFIND (Exact Match)	allow			
	BPROPPATCH	BPROPPATCH (Exact Match)	allow			
	NOTIFY	NOTIFY (Exact Match)	allow			
	POLL	POLL (Exact Match)	allow			
	SEARCH	SEARCH (Exact Match)	allow			
	SUBSCRIBE	SUBSCRIBE (Exact Match)	allow			
	UNSUBSCRIBE	UNSUBSCRIBE (Exact Match)	allow			
	CCM_POST	CCM_POST (Exact Match)	allow			
	MKACTIVITY	MKACTIVITY (Exact Match)	allow			
	CHECKOUT	CHECKOUT (Exact Match)	allow			
	MERGE	MERGE (Exact Match)	allow			
	REPORT	REPORT (Exact Match)	allow			
	CHECKIN	CHECKIN (Exact Match)	allow			
	UNCHECKOUT	UNCHECKOUT (Exact Match)	allow			
	UPDATE	UPDATE (Exact Match)	allow			
	LABEL	LABEL (Exact Match)	allow			
	VERSION-CONTROL	VERSION-CONTROL (Exact Match)	allow			
	BASELINE_CONTROL	BASELINE_CONTROL (Exact Match)	allow			
	MKWORKSPACE	MKWORKSPACE (Exact Match)	allow			
	{fallthrough}		allow	yes		

(webDAV plus extension is enabled)

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

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	From:*	From:* (Pattern Match)	allow			yes
	Via:*	Via:* (Pattern Match)	allow			yes
	Referer:*	Referer:* (Pattern Match)	allow			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			

HTTP Response

General Settings		
	Idle Timeout	10 minutes
	Maximum line length	4096 bytes
	Maximum total length	-

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

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	text/*	text/* (Pattern Match)	allow			
	image/*	image/* (Pattern Match)	allow			
	audio/*	audio/* (Pattern Match)	allow			
	application/pdf	application/pdf (Exact Match)	allow			
	application/x-javascript	application/x-javascript (Exact Match)	allow			
	application/x-shockwave-flash	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			
	application/x-rtsp-tunnelled	application/x-rtsp-tunnelled (Pattern Match)	allow			
	application/*	application/* (Pattern Match)	allow			
	(none)		allow			yes
	{fallthrough}		allow	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		yes
	ZIP archive	%0x504b0304%* (Pattern Match)	deny	yes		yes
	Windows EXE/DLL	%0x4d5a%* (Pattern Match)	deny	yes		
	Windows CAB archive	%0x4d53434600000000%* (Pattern Match)	deny	yes		yes
	{fallthrough}		allow			

Exceptions

*.airtightnetworks.com
*.cloudwifi.com
*.microsoft.com
*.mojonetworks.com
*.windows.com
*.windowsupdate.com
redirector.online.spectraguard.net

Webblocker

WebBlocker.1

Deny Message

Content-type: text/html; charset="utf-8"%CRLF%%CRLF%<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">%CRLF%<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">%CRLF% <head>%CRLF% <title>%(transaction)% denied by WatchGuard HTTP Proxy</title> %CRLF% <style type="text/css">%CRLF% body {%CRLF% font-family: Arial, Helvetica, Verdana, Sans-Serif;%CRLF% font-size: small; %CRLF% font-weight: normal; %CRLF% color: #000000;%CRLF% }%CRLF% div { %CRLF% margin-left: auto; %CRLF% margin-right: auto; %CRLF% text-align: center;%CRLF% }%CRLF% .box { %CRLF% width: 600px;%CRLF% background-color: #F2F2F2; %CRLF% border-left: solid 1px #C2C2C2; %CRLF% border-right: solid 1px #C2C2C2; %CRLF% vertical-align: middle;%CRLF% padding: 20px 10px 20px 10px;%CRLF% }%CRLF% p {%CRLF% text-align: left;%CRLF% }%CRLF% .red {%CRLF% font-weight: bold;%CRLF% color: Red;%CRLF% text-align: center;%CRLF% }%CRLF% .band { %CRLF% height: 20px;%CRLF% color: White;%CRLF% background: #333333;%CRLF% width: 600px;%CRLF% border-left: solid 1px #333333;%CRLF% border-right: solid 1px #333333;%CRLF% padding: 3px 10px 0px 10px;%CRLF% }%CRLF% div#wrap {%CRLF% margin-top: 50px;%CRLF% }%CRLF% </style>%CRLF% </head>%CRLF% <body> %CRLF% %CRLF% %CRLF% %CRLF% %(transaction)% denied by WatchGuard HTTP Proxy. %CRLF% Reason: %(reason)% %CRLF% Please contact your administrator for assistance. %CRLF% More Details: %CRLF% Method: %(method)% %CRLF% Host: %(url-host)% %CRLF% Path: %(url-path)% %CRLF% %CRLF% WatchGuard Technologies, Inc. %CRLF% %CRLF% </body>%CRLF%</html>

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

1.5.2.7 HTTP-Client.Standard.Outgoing.1

Created by Policy Manager

HTTP Request

General Settings	Idle Timeout	10 min
	Maximum URL length	4096 bytes
	Allow range requests through unmodified	enabled (Log: enabled)
	Enforce Safe Search	disabled
	Enable YouTube for Schools	disabled
	Logging for reports	enabled

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			
	COPY	COPY (Exact Match)	allow			
	LOCK	LOCK (Exact Match)	allow			
	MKCOL	MKCOL (Exact Match)	allow			
	MOVE	MOVE (Exact Match)	allow			
	PROPFIND	PROPFIND (Exact Match)	allow			
	PROPPATCH	PROPPATCH (Exact Match)	allow			
	UNLOCK	UNLOCK (Exact Match)	allow			
	BCOPY	BCOPY (Exact Match)	allow			
	BDELETE	BDELETE (Exact Match)	allow			
	BMOVE	BMOVE (Exact Match)	allow			
	BPROPFIND	BPROPFIND (Exact Match)	allow			
	BPROPPATCH	BPROPPATCH (Exact Match)	allow			
	NOTIFY	NOTIFY (Exact Match)	allow			
	POLL	POLL (Exact Match)	allow			
	SEARCH	SEARCH (Exact Match)	allow			
	SUBSCRIBE	SUBSCRIBE (Exact Match)	allow			
	UNSUBSCRIBE	UNSUBSCRIBE (Exact Match)	allow			
	CCM_POST	CCM_POST (Exact Match)	allow			
	MKACTIVITY	MKACTIVITY (Exact Match)	allow			
	CHECKOUT	CHECKOUT (Exact Match)	allow			
	MERGE	MERGE (Exact Match)	allow			
	REPORT	REPORT (Exact Match)	allow			
	CHECKIN	CHECKIN (Exact Match)	allow			
	UNCHECKOUT	UNCHECKOUT (Exact Match)	allow			
	UPDATE	UPDATE (Exact Match)	allow			
	LABEL	LABEL (Exact Match)	allow			
	VERSION-CONTROL	VERSION-CONTROL (Exact Match)	allow			
	BASELINE_CONTROL	BASELINE_CONTROL (Exact Match)	allow			
	MKWORKSPACE	MKWORKSPACE (Exact Match)	allow			
	{fallthrough}		allow	yes		

(webDAV plus extension is enabled)

URL Paths	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		AV scan			

Header Fields	Name	Rule	Action	Logging	Alarm	Disabled
	From:*	From:* (Pattern Match)	allow			yes
	Via:*	Via:* (Pattern Match)	allow			yes
	Referer:*	Referer:* (Pattern Match)	allow			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			

HTTP Response

General Settings		
	Idle Timeout	10 minutes
	Maximum line length	4096 bytes
	Maximum total length	-

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

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	text/*	text/* (Pattern Match)	AV scan			
	image/*	image/* (Pattern Match)	AV scan			
	audio/*	audio/* (Pattern Match)	AV scan			
	application/pdf	application/pdf (Exact Match)	AV scan			
	application/x-javascript	application/x-javascript (Exact Match)	AV scan			
	application/x-shockwave-flash	application/x-shockwave-flash (Exact Match)	AV scan			
	application/*xml*	application/*xml* (Pattern Match)	AV scan			
	application/x-httpd-*	application/x-httpd-* (Pattern Match)	AV scan			
	httpd/*	httpd/* (Pattern Match)	AV scan			
	application/x-rtsp-tunnelled	application/x-rtsp-tunnelled (Pattern Match)	AV scan			
	application/*	application/* (Pattern Match)	AV scan			
	(none)		allow			yes
	{fallthrough}		AV scan	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		yes
	ZIP archive	%0x504b0304%* (Pattern Match)	deny	yes		yes
	Windows EXE/DLL	%0x4d5a%* (Pattern Match)	deny	yes		
	Windows CAB archive	%0x4d53434600000000%* (Pattern Match)	deny	yes		yes
	{fallthrough}		AV scan			

Exceptions

*.airtightnetworks.com
*.cloudwifi.com
*.microsoft.com
*.mojonetworks.com
*.windows.com
*.windowsupdate.com
redirector.online.spectraguard.net

Webblocker

WebBlocker.1

AntiVirus	Name	Action	Logging	Alarm
	Virus found	drop	yes	
	Unable to scan	allow	yes	
	Limit scanning	1024 kilobyte(s)		

Deny Message

Content-type: text/html; charset="utf-8"%CRLF%%CRLF%<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">%CRLF%<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">%CRLF% <head>%CRLF% <title>%(transaction)% denied by WatchGuard HTTP Proxy</title> %CRLF% <style type="text/css">%CRLF% body {%CRLF% font-family: Arial, Helvetica, Verdana, Sans-Serif;%CRLF% font-size: small; %CRLF% font-weight: normal; %CRLF% color: #000000;%CRLF% }%CRLF% div { %CRLF% margin-left: auto; %CRLF% margin-right: auto; %CRLF% text-align: center;%CRLF% }%CRLF% .box { %CRLF% width: 600px;%CRLF% background-color: #F2F2F2; %CRLF% border-left: solid 1px #C2C2C2; %CRLF% border-right: solid 1px #C2C2C2; %CRLF% vertical-align: middle;%CRLF% padding: 20px 10px 20px 10px;%CRLF% }%CRLF% p {%CRLF% text-align: left;%CRLF% }%CRLF% .red {%CRLF% font-weight: bold;%CRLF% color: Red;%CRLF% text-align: center;%CRLF% }%CRLF% .band { %CRLF% height: 20px;%CRLF% color: White;%CRLF% background: #333333;%CRLF% width: 600px;%CRLF% border-left: solid 1px #333333;%CRLF% border-right: solid 1px #333333;%CRLF% padding: 3px 10px 0px 10px;%CRLF% }%CRLF% div#wrap {%CRLF% margin-top: 50px;%CRLF% }%CRLF% </style>%CRLF% </head>%CRLF% <body> %CRLF% %CRLF% %CRLF% %CRLF% %(transaction)% denied by WatchGuard HTTP Proxy. %CRLF% Reason: %(reason)% %CRLF% Please contact your administrator for assistance. %CRLF% More Details: %CRLF% Method: %(method)% %CRLF% Host: %(url-host)% %CRLF% Path: %(url-path)% %CRLF% %CRLF% WatchGuard Technologies, Inc. %CRLF% %CRLF% </body>%CRLF%</html>

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.2.8 HTTP-Server.Standard.Web-Server

WatchGuard recommended standard configuration for HTTP-Server with logging enabled

HTTP Request

General Settings	Idle Timeout	10 min
	Maximum URL length	2048 bytes
	Allow range requests through unmodified	disabled (Log: disabled)
	Enforce Safe Search	disabled
	Enable YouTube for Schools	disabled
	Logging for reports	enabled

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
	COPY	COPY (Exact Match)	allow			
	LOCK	LOCK (Exact Match)	allow			
	MKCOL	MKCOL (Exact Match)	allow			
	MOVE	MOVE (Exact Match)	allow			
	PROPFIND	PROPFIND (Exact Match)	allow			
	PROPPATCH	PROPPATCH (Exact Match)	allow			
	UNLOCK	UNLOCK (Exact Match)	allow			
	BCOPY	BCOPY (Exact Match)	allow			
	BDELETE	BDELETE (Exact Match)	allow			
	BMOVE	BMOVE (Exact Match)	allow			
	BPROPFIND	BPROPFIND (Exact Match)	allow			
	BPROPPATCH	BPROPPATCH (Exact Match)	allow			
	NOTIFY	NOTIFY (Exact Match)	allow			
	POLL	POLL (Exact Match)	allow			
	SEARCH	SEARCH (Exact Match)	allow			
	SUBSCRIBE	SUBSCRIBE (Exact Match)	allow			
	UNSUBSCRIBE	UNSUBSCRIBE (Exact Match)	allow			
	CCM_POST	CCM_POST (Exact Match)	allow			
	MKACTIVITY	MKACTIVITY (Exact Match)	allow			
	CHECKOUT	CHECKOUT (Exact Match)	allow			
	MERGE	MERGE (Exact Match)	allow			
	REPORT	REPORT (Exact Match)	allow			
	CHECKIN	CHECKIN (Exact Match)	allow			
	UNCHECKOUT	UNCHECKOUT (Exact Match)	allow			
	UPDATE	UPDATE (Exact Match)	allow			
	LABEL	LABEL (Exact Match)	allow			
	VERSION-CONTROL	VERSION-CONTROL (Exact Match)	allow			
	BASELINE_CONTROL	BASELINE_CONTROL (Exact Match)	allow			
	MKWORKSPACE	MKWORKSPACE (Exact Match)	allow			
	{fallthrough}		deny	yes		

(webDAV plus extension is enabled)

URL Paths	Name	Rule	Action	Logging	Alarm	Disabled
	www.demo.com	www.demo.com/* (Pattern Match)	AV scan	yes		
	{fallthrough}		deny	yes		

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			

HTTP Response

General Settings	Idle Timeout	10 minutes
	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}		AV scan	yes		

Cookies	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

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

Exceptions

AntiVirus	Name	Action	Logging	Alarm
	Virus found	drop	yes	
	Unable to scan	allow	yes	
	Limit scanning	1024 kilobyte(s)		

Deny Message

Content-type: text/html; charset="utf-8"%CRLF%%CRLF%<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">%CRLF%<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">%CRLF% <head>%CRLF% <title>%(transaction)% denied by WatchGuard HTTP Proxy</title> %CRLF% <style type="text/css">%CRLF% body {%CRLF% font-family: Arial, Helvetica, Verdana, Sans-Serif;%CRLF% font-size: small; %CRLF% font-weight: normal; %CRLF% color: #000000;%CRLF% }%CRLF% div { %CRLF% margin-left: auto; %CRLF% margin-right: auto; %CRLF% text-align: center;%CRLF% }%CRLF% .box { %CRLF% width: 600px;%CRLF% background-color: #F2F2F2; %CRLF% border-left: solid 1px #C2C2C2; %CRLF% border-right: solid 1px #C2C2C2; %CRLF% vertical-align: middle;%CRLF% padding: 20px 10px 20px 10px;%CRLF% }%CRLF% p {%CRLF% text-align: left;%CRLF% }%CRLF% .red {%CRLF% font-weight: bold;%CRLF% color: Red;%CRLF% text-align: center;%CRLF% }%CRLF% .band { %CRLF% height: 20px;%CRLF% color: White;%CRLF% background: #333333;%CRLF% width: 600px;%CRLF% border-left: solid 1px #333333;%CRLF% border-right: solid 1px #333333;%CRLF% padding: 3px 10px 0px 10px;%CRLF% }%CRLF% div#wrap {%CRLF% margin-top: 50px;%CRLF% }%CRLF% </style>%CRLF% </head>%CRLF% <body> %CRLF% %CRLF% %CRLF% %CRLF% %(transaction)% denied by WatchGuard HTTP Proxy. %CRLF% Reason: %(reason)% %CRLF% Please contact your administrator for assistance. %CRLF% More Details: %CRLF% Method: %(method)% %CRLF% Host: %(url-host)% %CRLF% Path: %(url-path)% %CRLF% %CRLF% WatchGuard Technologies, Inc. %CRLF% %CRLF% </body>%CRLF%</html>

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.2.9 HTTP-Server.Standard.Web-Server.1

Created by Policy Manager

HTTP Request

General Settings	Idle Timeout	10 min
	Maximum URL length	2048 bytes
	Allow range requests through unmodified	disabled (Log: disabled)
	Enforce Safe Search	disabled
	Enable YouTube for Schools	disabled
	Logging for reports	enabled

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
	COPY	COPY (Exact Match)	allow			
	LOCK	LOCK (Exact Match)	allow			
	MKCOL	MKCOL (Exact Match)	allow			
	MOVE	MOVE (Exact Match)	allow			
	PROPFIND	PROPFIND (Exact Match)	allow			
	PROPPATCH	PROPPATCH (Exact Match)	allow			
	UNLOCK	UNLOCK (Exact Match)	allow			
	BCOPY	BCOPY (Exact Match)	allow			
	BDELETE	BDELETE (Exact Match)	allow			
	BMOVE	BMOVE (Exact Match)	allow			
	BPROPFIND	BPROPFIND (Exact Match)	allow			
	BPROPPATCH	BPROPPATCH (Exact Match)	allow			
	NOTIFY	NOTIFY (Exact Match)	allow			
	POLL	POLL (Exact Match)	allow			
	SEARCH	SEARCH (Exact Match)	allow			
	SUBSCRIBE	SUBSCRIBE (Exact Match)	allow			
	UNSUBSCRIBE	UNSUBSCRIBE (Exact Match)	allow			
	CCM_POST	CCM_POST (Exact Match)	allow			
	MKACTIVITY	MKACTIVITY (Exact Match)	allow			
	CHECKOUT	CHECKOUT (Exact Match)	allow			
	MERGE	MERGE (Exact Match)	allow			
	REPORT	REPORT (Exact Match)	allow			
	CHECKIN	CHECKIN (Exact Match)	allow			
	UNCHECKOUT	UNCHECKOUT (Exact Match)	allow			
	UPDATE	UPDATE (Exact Match)	allow			
	LABEL	LABEL (Exact Match)	allow			
	VERSION-CONTROL	VERSION-CONTROL (Exact Match)	allow			
	BASELINE_CONTROL	BASELINE_CONTROL (Exact Match)	allow			
	MKWORKSPACE	MKWORKSPACE (Exact Match)	allow			
	{fallthrough}		deny	yes		

(webDAV plus extension is enabled)

URL Paths	Name	Rule	Action	Logging	Alarm	Disabled
	www.demo.com	www.demo.com/* (Pattern Match)	AV scan	yes		
	{fallthrough}		deny	yes		

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			

HTTP Response

General Settings	Idle Timeout	10 minutes
	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}		AV scan	yes		

Cookies	Name	Rule	Action	Logging	Alarm	Disabled
	{fallthrough}		allow			

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

Exceptions

AntiVirus	Name	Action	Logging	Alarm
	Virus found	drop	yes	
	Unable to scan	allow	yes	
	Limit scanning	1024 kilobyte(s)		

Deny Message

Content-type: text/html; charset="utf-8"%CRLF%%CRLF%<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">%CRLF%<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">%CRLF% <head>%CRLF% <title>%(transaction)% denied by WatchGuard HTTP Proxy</title> %CRLF% <style type="text/css">%CRLF% body {%CRLF% font-family: Arial, Helvetica, Verdana, Sans-Serif;%CRLF% font-size: small; %CRLF% font-weight: normal; %CRLF% color: #000000;%CRLF% }%CRLF% div { %CRLF% margin-left: auto; %CRLF% margin-right: auto; %CRLF% text-align: center;%CRLF% }%CRLF% .box { %CRLF% width: 600px;%CRLF% background-color: #F2F2F2; %CRLF% border-left: solid 1px #C2C2C2; %CRLF% border-right: solid 1px #C2C2C2; %CRLF% vertical-align: middle;%CRLF% padding: 20px 10px 20px 10px;%CRLF% }%CRLF% p {%CRLF% text-align: left;%CRLF% }%CRLF% .red {%CRLF% font-weight: bold;%CRLF% color: Red;%CRLF% text-align: center;%CRLF% }%CRLF% .band { %CRLF% height: 20px;%CRLF% color: White;%CRLF% background: #333333;%CRLF% width: 600px;%CRLF% border-left: solid 1px #333333;%CRLF% border-right: solid 1px #333333;%CRLF% padding: 3px 10px 0px 10px;%CRLF% }%CRLF% div#wrap {%CRLF% margin-top: 50px;%CRLF% }%CRLF% </style>%CRLF% </head>%CRLF% <body> %CRLF% %CRLF% %CRLF% %CRLF% %(transaction)% denied by WatchGuard HTTP Proxy. %CRLF% Reason: %(reason)% %CRLF% Please contact your administrator for assistance. %CRLF% More Details: %CRLF% Method: %(method)% %CRLF% Host: %(url-host)% %CRLF% Path: %(url-path)% %CRLF% %CRLF% WatchGuard Technologies, Inc. %CRLF% %CRLF% </body>%CRLF%</html>

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.2.10 HTTPS-Client.Standard.Outgoing

WatchGuard recommended standard configuration for HTTPS-Client with logging enabled

Content Inpection

Deep inspection of HTTPS content	enabled
Proxy Action	HTTP-Client.Standard.Outgoing
Use OCSP for certificate validation	enabled
Certificates which cannot be validated are	valid
Perfect Forward Secrecy Ciphers	Allowed

Domain Names	Name	Rule	Action	Logging	Alarm	Disabled
	WatchGuard Services	*.watchguard.com (Pattern Match)	allow			
	*.mojonetworks.com	*.mojonetworks.com (Pattern Match)	allow			
	*.cloudwifi.com	*.cloudwifi.com (Pattern Match)	allow			
	redirector.online.spectragua...	redirector.online.spectraguard.net (Pattern Match)	allow			
	*.airtightnetworks.com	*.airtightnetworks.com (Pattern Match)	allow			
	{fallthrough}		allow			

Webblocker & General Settings

Webblocker	WebBlocker.2
Allow only SSL compliant traffic	disabled
Idle Timeout	10 min
Logging for reports	enabled

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

1.5.2.11 POP3-Client.Standard.1

Created by Policy Manager

General

General Settings	Idle Timeout	1 min
	Maximum email line length	1000 bytes
	Hide email Server replies	enabled
	Allow uuencoded attachments	enabled
	Allow BinHex attachments	enabled
	Turn on logging for reports	enabled

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			
	NTLM	NTLM (Exact Match)	allow			
	LOGIN	LOGIN (Exact Match)	allow			
	GSSAPI	GSSAPI (Exact Match)	allow			
	KERBEROS_V4	KERBEROS_V4 (Exact Match)	allow			
	{fallthrough}		deny	yes		

Attachments

Content Types	Name	Rule	Action	Logging	Alarm	Disabled
	All text types	text/* (Pattern Match)	AV scan			
	All image types	image/* (Pattern Match)	AV scan			
	All audio types	audio/* (Pattern Match)	AV scan			
	All video types	video/* (Pattern Match)	AV scan			
	All multi-part MIME types	multipart/* (Pattern Match)	AV scan			
	Message parts	message/* (Pattern Match)	AV scan			
	Missing or empty		AV scan			
	{fallthrough}		AV scan	yes		

Filenames	Name	Rule	Action	Logging	Alarm	Disabled
	Text files	*.txt (Pattern Match)	AV scan			
	Word documents	*.doc (Pattern Match)	AV scan			
	Excel spreadsheets	*.xls (Pattern Match)	AV scan			
	Missing or empty		AV scan			
	{fallthrough}		AV scan	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-Encoding:*	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			
	Priority:*	Priority:* (Pattern Match)	allow			
	Return-Receipt-To:*	Return-Receipt-To:* (Pattern Match)	allow			
	X-WatchGuard-Spam-ID:*	X-WatchGuard-Spam-ID:* (Pattern Match)	allow			
	X-WatchGuard-Mail-From:*	X-WatchGuard-Mail-From:* (Pattern Match)	allow			
	X-WatchGuard-Mail-Recipie...	X-WatchGuard-Mail-Recipients:* (Pattern Match)	allow			yes
	X-WatchGuard-Mail-Excepti...	X-WatchGuard-Mail-Exception:* (Pattern Match)	allow			
	X-WatchGuard-Spam-Score:*	X-WatchGuard-Spam-Score:* (Pattern Match)	allow			
	X-WatchGuard-Mail-Client-I...	X-WatchGuard-Mail-Client-IP:* (Pattern Match)	allow			
	X-Mailer:*	X-Mailer:* (Pattern Match)	allow			
	{fallthrough}		allow	yes		

AntiVirus	**Name**	**Action**	**Logging**	**Alarm**
	When a virus is detected	strip/remove	yes	
	When a scan error occurs	strip/remove	yes	
	Limit scanning	1024 kilobyte(s)		

spamBlocker	**Name**	**Action**	**Logging**
	Spam	replace with: ***SPAM***	yes
	Bulk	replace with: ***BULK***	yes
	Suspect	replace with: ***SUSPECT***	yes

When the spamBlocker server is unavailabe, access to POP3 email is: allow
Send a log message for each email classified as not spam: yes

VOD	Action	Alarm	Log
Virus found	strip/remove		yes
Unable to scan	strip/remove		yes

Deny Message

The WatchGuard Firebox that protects your network has detected a message that 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%Recovery : %(recovery)%%CRLF%%CRLF%

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.2.12 SMTP-Incoming.Standard.1

Created by Policy Manager

General

General Settings	Idle Timeout	10 min
	Maximum email recipients	99
	Maximum address length	-
	Maximum email size	20000 kilobytes
	Maximum email line length	1000 bytes
	Maximum email header size	bytes
	Hide email server	by masquerading of Server-replies ()
	Allow uuencoded attachments	enabled
	Allow BinHex attachments	enabled
	Auto-block source of invalid commands	enabled
	Log message for a denied SMTP command	disabled
	Logging for reports	enabled

Greeting Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Non-allowed characters	[^-.0-9a-zA-Z_\[\]] (RegExp)	deny	yes		
	Maximum length	^.{513,}$ (RegExp)	deny	yes		
	{fallthrough}		allow			

ESMTP

ESMTP Settings	Allow BDAT/CHUNKING	no
	Allow ETRN	yes
	Allow 8-Bit MIME	yes
	Allow Binary MIME	no
	Log denied ESMTP options	yes
SMTP with TLS	disabled	

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)	AV scan			
	image/*	image/* (Pattern Match)	AV scan			
	multipart/*	multipart/* (Pattern Match)	AV scan			
	message/*	message/* (Pattern Match)	AV scan			
	application/*	application/* (Pattern Match)	AV scan			
	(none)		AV scan			
	application/x-watchguard-lo...	application/x-watchguard-locked (Exact Match)	allow			yes
	{fallthrough}		AV scan	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}		AV scan			

Addresses

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

Rcpt To Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Source-routed addresses	*!*@* (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-Encoding:*	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			
	Priority:*	Priority:* (Pattern Match)	allow			
	Return-Receipt-To:*	Return-Receipt-To:* (Pattern Match)	allow			
	X-WatchGuard-Spam-ID:*	X-WatchGuard-Spam-ID:* (Pattern Match)	allow			
	X-WatchGuard-Mail-From:*	X-WatchGuard-Mail-From:* (Pattern Match)	allow			
	X-WatchGuard-Mail-Recipie...	X-WatchGuard-Mail-Recipients:* (Pattern Match)	allow			yes
	X-WatchGuard-Mail-Excepti...	X-WatchGuard-Mail-Exception:* (Pattern Match)	allow			
	X-WatchGuard-Spam-Score:*	X-WatchGuard-Spam-Score:* (Pattern Match)	allow			
	X-WatchGuard-Mail-Client-I...	X-WatchGuard-Mail-Client-IP:* (Pattern Match)	allow			
	X-Mailer:*	X-Mailer:* (Pattern Match)	allow			
	{fallthrough}		allow			

AntiVirus	Name	Action	Logging	Alarm
	Virus found	strip/remove	yes	
	Unable to scan	lock	yes	
	Limit scanning	1024 kilobyte(s)		

spamBlocker	Name	Action	Logging
disabled			

Deny Message

The WatchGuard Firebox that protects your network has detected a message that may not be safe.%CRLF%%CRLF%Cause : %(reason)%%CRLF%Content type : %(type)%%CRLF%File name : %(filename)%%CRLF%Status : %(virus)%%CRLF%Action : The Firebox %(action)% %(filename)%.%CRLF%%CRLF%Your network administrator %(recovery)% this attachment.%CRLF%%CRLF%

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.2.13 SMTP-Incoming.Standard.Mail-Server

WatchGuard recommended standard configuration for SMTP-Incoming with logging enabled

General

General Settings	Idle Timeout	10 min
	Maximum email recipients	99
	Maximum address length	-
	Maximum email size	20000 kilobytes
	Maximum email line length	1000 bytes
	Maximum email header size	20000 bytes
	Hide email server	by masquerading of Server-replies ()
	Allow uuencoded attachments	enabled
	Allow BinHex attachments	enabled
	Auto-block source of invalid commands	enabled
	Log message for a denied SMTP command	disabled
	Logging for reports	enabled

Greeting Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Non-allowed characters	[^-.0-9a-zA-Z_\[\]] (RegExp)	deny	yes		
	Maximum length	^.{513,}$ (RegExp)	deny	yes		
	{fallthrough}		allow			

ESMTP

ESMTP Settings	Allow BDAT/CHUNKING	no
	Allow ETRN	yes
	Allow 8-Bit MIME	yes
	Allow Binary MIME	no
	Log denied ESMTP options	yes
SMTP with TLS	disabled	

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)	AV scan			
	image/*	image/* (Pattern Match)	AV scan			
	multipart/*	multipart/* (Pattern Match)	AV scan			
	message/*	message/* (Pattern Match)	AV scan			
	application/*	application/* (Pattern Match)	AV scan			
	(none)		AV scan			
	application/x-watchguard-lo...	application/x-watchguard-locked (Exact Match)	allow			yes
	{fallthrough}		AV scan	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}		AV scan			

Addresses

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

Rcpt To Rules	Name	Rule	Action	Logging	Alarm	Disabled
	Source-routed addresses	*!*@* (Pattern Match)	deny			
	Non-allowed characters	[^-_'.+=%*/#$^`{|}~!&@?0-9a-zA-Z] (RegExp)	deny			
	demo.com	*@demo.com (Pattern Match)	allow	yes		
	{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-Encoding:*	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			
	Priority:*	Priority:* (Pattern Match)	allow			
	Return-Receipt-To:*	Return-Receipt-To:* (Pattern Match)	allow			
	X-WatchGuard-Spam-ID:*	X-WatchGuard-Spam-ID:* (Pattern Match)	allow			
	X-WatchGuard-Mail-From:*	X-WatchGuard-Mail-From:* (Pattern Match)	allow			
	X-WatchGuard-Mail-Recipie...	X-WatchGuard-Mail-Recipients:* (Pattern Match)	allow			yes
	X-WatchGuard-Mail-Excepti...	X-WatchGuard-Mail-Exception:* (Pattern Match)	allow			
	X-WatchGuard-Spam-Score:*	X-WatchGuard-Spam-Score:* (Pattern Match)	allow			
	X-WatchGuard-Mail-Client-I...	X-WatchGuard-Mail-Client-IP:* (Pattern Match)	allow			
	X-Mailer:*	X-Mailer:* (Pattern Match)	allow			
	{fallthrough}		allow			

Add X-Watchguard headers enabled

AntiVirus	Name	Action	Logging	Alarm
	Virus found	strip/remove	yes	
	Unable to scan	lock	yes	
	Limit scanning	1024 kilobyte(s)		

spamBlocker	Name	Action	Logging

disabled

Deny Message

The WatchGuard Firebox that protects your network has detected a message that may not be safe.%CRLF%%CRLF%Cause : %(reason)%%CRLF%Content type : %(type)%%CRLF%File name : %(filename)%%CRLF%Status : %(virus)%%CRLF%Action : The Firebox %(action)% %(filename)%.%CRLF%%CRLF%Your network administrator %(recovery)% this attachment.%CRLF%%CRLF%

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

APT Blocker	enabled

1.5.3 Webblocker

WebBlocker.1

Description	Default configuration for WebBlocker
Categories from	Websense cloud

Denied Categories				Logging	Alarm if denied	
	Adult Content, Adult Material, Advanced Malware Command and Control, Bot Networks, Compromised Websites, Dynamic DNS, Elevated Exposure, Emerging Exploits, Extended Protection, Gambling, Games, Keyloggers, Lingerie and Swimsuit, Malicious Embedded Link, Malicious Embedded iFrame, Malicious Web Sites, Mobile Malware, Newly Registered Websites, Nudity, Phishing and Other Frauds, Potentially Damaging Content, Potentially Unwanted Software, Security, Sex, Sex Education, Spyware, Suspicious Embedded Link			yes		
Exceptions	**Name**	**Rule**	**Action**	**Logging**	**Alarm**	**Disabled**
	update DB	listsrv.surfcontrol.com/* (Pattern Match)	allow			
	WatchGuard	^[0-9a-zA-Z_\-.]{1,256}\.watchguard\.com/ (RegExp)	allow			
	{fallthrough}		allow			

Advanced	
Local override	disabled
Cache Size	100 entries
Server Timeout	in 5 seconds (log enabled)
Action at sServer timeout	deny access (log enabled)
When license expires	access to websites is denied

WebBlocker.2

Description	Default configuration for WebBlocker
Categories from	Websense cloud

Denied Categories				Logging	Alarm if denied	
	Adult Content, Adult Material, Advanced Malware Command and Control, Bot Networks, Compromised Websites, Dynamic DNS, Elevated Exposure, Emerging Exploits, Extended Protection, Gambling, Games, Keyloggers, Lingerie and Swimsuit, Malicious Embedded Link, Malicious Embedded iFrame, Malicious Web Sites, Mobile Malware, Newly Registered Websites, Nudity, Phishing and Other Frauds, Potentially Damaging Content, Potentially Unwanted Software, Security, Sex, Sex Education, Spyware, Suspicious Embedded Link			yes		
Exceptions	**Name**	**Rule**	**Action**	**Logging**	**Alarm**	**Disabled**
	update DB	listsrv.surfcontrol.com/* (Pattern Match)	allow			
	WatchGuard	^[0-9a-zA-Z_\-.]{1,256}\.watchguard\.com/ (RegExp)	allow			
	{fallthrough}		allow			

Advanced	
Local override	disabled
Cache Size	100 entries
Server Timeout	in 5 seconds (log enabled)
Action at sServer timeout	deny access (log enabled)
When license expires	access to websites is denied

1.5.4 Schedules

Always On

	Sun-Sat	0:00-24:00

MF 0700-1900

Description	Monday through Friday 7AM to 7PM	
	Monday	7:00-19:00
	Tuesday	7:00-19:00
	Wednesday	7:00-19:00
	Thursday	7:00-19:00
	Friday	7:00-19:00

Non Working Hours

Sunday	0:00-8:00, 12:00-14:00, 18:00-24:00
Monday	0:00-8:00, 12:00-14:00, 18:00-24:00
Tuesday	0:00-8:00, 12:00-14:00, 18:00-24:00
Wednesday	0:00-8:00, 12:00-14:00, 18:00-24:00
Thursday	0:00-8:00, 12:00-14:00, 18:00-24:00
Friday	0:00-8:00, 12:00-14:00, 18:00-24:00
Saturday	0:00-8:00, 12:00-14:00, 18:00-24:00

1.5.5 SNAT

Static NAT	External IP	Source IP	Internal IP:Port
DNS_Server_WAN1	194.86.213.45		10.0.4.53
DNS_Server_WAN2	43.14.57.145		10.0.4.53
Mail-Server_WAN2	43.14.57.145		10.0.4.25

Server Load Balancing	External IP	Source IP	Internal IP:Port	Weight
Web-Server_WAN1_Cluster (Round-robin)	194.86.213.45		10.0.4.80	1
			10.0.4.81	1
Web-Server_WAN2-Cluster (Round-robin)	43.14.57.145		10.0.4.80	1
			10.0.4.81	1

1.5.6 Quotas

Rules	User and group	Action	Enabled	Description
Surf_Users	surf_users	5Mb	enabled	

Actions	Bandwidth [MB/day]	Time [min/day]	Description
5Mb	5	0	

1.5.6.1 Quota Exceptions

Exceptions

10.0.1.15

1.6 Default Threat Protection

1.6.1 Default Packet Handling

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

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

DDOS Prevention	Settings
Per Server Quota	enabled - Threshold: 100 connections/sec
Per Client Quota	enabled - Threshold: 300 connections/sec

Logging of Dangerous Activities	
IP Spoofing Attacks	Log
ARP Spoofing Attacks	Log
Port Probes	Log
Address Space Probes	Log
IP Source Route	Log
Ping of Death	Log
IPSec Flood Attack	Log
IKE Flood Attack	Log
SYN Flood Attack	Log
ICMP Flood Attack	Log
UDP Flood Attack	Log
DDOS Attack Destination	Log
DDOS Attack Source	Log
Incoming Broadcast	
Outgoing Broadcast	
Unhandled Internal Packet	Log
Unhandled External Packet	Log

1.6.2 Blocked Sites

Logging & Notification: Log
Duration for Auto-Blocked Sites: 20 Minutes

1.6.3 Blocked Ports

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

1.7 NTP

NTP

Use NTP to synchronize system time	enabled, Server: 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org

1.8 SNMP

SNMP

Polling	v1/v2 - Community String:
Traps	disabled

1.9 Global Settings

Global Settings

General		
WebUI Port	8080	
Automatic Reboot	disabled	
Send device feedback to WG	enabled	
Send Fault Reports to WG daily	disabled	
Allow more than one Device Admin	enabled	
Networking		
ICMP Error Handling	Fragmentation Req (PMTU)	enabled
	Time Exceeded	enabled
	Network Unreachable	enabled
	Host Unreachable	enabled
	Port Unreachable	enabled
	Protocol Unreachable	enabled
TCP SYN packet / connection state	TCP SYN packet and connection state verification	enabled
	TCP connection timeout	3600 sec
TCP Maximum Segment Size Adjustment	TCP MSS Adjustment	Auto Adjustment
Traffic Management and QoS	Enable all traffic management and QoS features	enabled
Traffic Flow	Clear active connections when an SNAT action changes	disabled
Logon Disclaimer		
Logon Disclaimer	disabled	

1.10 OS Compatibility

OS Compatibility

For Fireware XTM version	11.9 or higher

2. Network Configuration

2.1 Interface List

No.	Name	Type	IP Address	MTU	Link-Speed	Description
0	WAN1 - Cable	External	DHCP (194.86.213.45)	1492	auto	Cable Provider
1	WAN2 - Fibre	External (sec. IP)	43.14.57.144/27 43.14.57.145/28	1500	auto	Fibre provider
2	LAN1	Trusted	10.0.1.1/24	1500	auto	Internal LAN
3	VOIP	Custom	172.16.1.1/24	1500	auto	Subnet for VOIP
4	DMZ	Optional	10.0.4.1/24	1500	auto	DMZ Subnet
5	AP1	Bridge		1500	auto	
6	AP2	Bridge		1500	auto	
7	VLAN Trunk	VLAN		1500	auto	
8	Optional-7	Cluster		1500	auto	
9	Optional-8	Cluster		1500	auto	

2.1.1 PPPoE & DHCP Client Configuration of Interfaces

No.	Name	Type	Parameter	Values
0	WAN1 - Cable	DHCP	IP	Use IP address: 194.86.213.45

2.1.2 Interface Settings for Traffic Management

No.	Name	Traffic Management	QoS	Prioritize Traffic	DF Bit	PMTU Settings
0	WAN1 - Cable	physical link speed	IP Precedence / Preserve		Copy	576bytes / 10min
1	WAN2 - Fibre	physical link speed	IP Precedence / Preserve		Copy	576bytes / 10min
2	LAN1	physical link speed	IP Precedence / Preserve			
3	VOIP	physical link speed	IP Precedence / Preserve			
4	DMZ	physical link speed	IP Precedence / Preserve			
5	AP1	physical link speed	IP Precedence / Preserve			
6	AP2	physical link speed	IP Precedence / Preserve			
7	VLAN Trunk	physical link speed	IP Precedence / Preserve			
8	Optional-7	physical link speed	IP Precedence / Preserve			
9	Optional-8	physical link speed	IP Precedence / Preserve			

2.2 Bridge

Name (Alias)	Zone	IP Address	DHCP	Interfaces	Description
AccessPoints	Custom	10.0.30.1/24	disabled	AP1, AP2	

2.3 VLAN

ID	Name (Alias)	Zone	IP Address	DHCP	Interfaces	Description
1	VLAN1 MGMT	Trusted	192.168.1.1/24	disabled	VLAN Trunk*	
40	VLAN40	Trusted	192.168.40.1/24	disabled	VLAN Trunk	
50	VLAN50	Trusted	192.168.50.1/24	disabled	VLAN Trunk	
80	VLAN80	Trusted	192.168.80.1/24	disabled	VLAN Trunk	

*) untagged traffic of this interface is assigned to this VLAN

2.4 Loopback Interface

	Name	IP Address	Description
	WG-Loopback	0.0.0.0/32	

2.5 DHCP Server Configuration

IF-No.	Name	Values	
2	LAN1	DHCP Ranges	10.0.1.100-10.0.1.200
		Lease Time	8 hours
		Reserved Addresses	Printer1:10.0.1.120-01:0F:23:77:AB:1D
		Domain	demo.local
		DNS Server	10.0.1.53
3	VOIP	DHCP Ranges	172.16.1.10-172.16.1.30
		Lease Time	7 days
		Domain	voip.demo.local
		DNS Server	172.16.1.53
		DHCP Options	TFTP Server Name (Code 66): pbx.voip.demo.local (Type: Text, Kind: Predefined)
			TFTP Boot Filename (Code 67): phones.img (Type: Text, Kind: Predefined)

2.6 WINS/DNS

Parameter	Value
Domain Name	
DNS Server	
WINS Server	,

2.7 Multi-WAN

Multi-WAN with Routing table

WAN1 - Cable
WAN2 - Fibre

2.7.1 Link Monitor

External Interface	Ping Monitor	TCP Monitor	Both Monitors?	Probe Interval	Deactivate after	Reactivate after
WAN1 - Cable	8.8.8.8			15	3	3
WAN2 - Fibre	8.8.4.4			15	3	3

2.7.2 Advanced Settings

Advanced Settings

Sticky Connection	TCP	0 seconds
	UDP	0 seconds
	Others	0 seconds
Failback for active Connections	Immediate failback	
Logging & Notification		

2.8 Network Address Translation

2.8.1 Dynamic NAT

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

2.9 Routing

2.9.1 Static Routes

Destination/Netmask		Gateway	Metric
10.0.18.0/255.255.255.0	->	10.0.4.254	1
172.23.0.0/255.255.255.0	->	Remote2	10

2.10 Gateway Wireless Controller

2.10.1 Settings

Gateway Wireless Controller	enabled
Access Point Settings	
Automatic update of AP firmware	enabled
Send AP log messages to Syslog server	disabled
Logging for reports	enabled
Management VLAN tagging	disabled
Wireless Scan Interval	1h
Location of AP devices	United States
SSH access on all Watchguard APs	disabled
Alarm Notification when AP goes offline	disabled
Alarm Notification when a Rogue AP is detected	disabled
Discovery Broadcasts	
Broadcast on all interfaces	enabled

2.10.2 SSID list

Work

Settings	
Broadcast SSID	enabled
Station Isolation	disabled
Use MAC ACL from Wireless Controller	disabled
VLAN tagging	disabled
Security	
Security Mode	WPA Enterprise, Encryption: TKIP or AES, Key Update Interval: 3600 Radius Server: 10.0.4.8:1812, Fast Roaming: disabled
Access Points	
Access Points with this SSID	AP320(radio1), AP320(radio2)

Guest-Access

Settings	
Broadcast SSID	enabled
Station Isolation	disabled
Use MAC ACL from Wireless Controller	disabled
VLAN tagging	VLAN ID: 80
Security	
Security Mode	Security Mode: WPA2 only (PSK), Encryption: TKIP or AES, Key Update Interval: 3600 sec
Access Points	
Access Points with this SSID	AP320(radio1)

2.10.3 AP list

AP320

Model	Model-No. 320
Serial number	3123456789012
Log to Syslog Server	disabled
Management VLAN tagging	enabled - VLAN ID: 1
Disable LEDs	disabled
Use outdoor channels only	disabled
Disable DFS Channels	disabled
Fast Handover	disabled
Band Steering	disabled

Network Settings	**DHCP**

Radio1

Band	2.4 GHz
Wireless Mode	802.11 G/N
Preferred Channel	Auto
Channel HT Mode	20 MHz
Extension Channel	Upper Channel
Rate	Auto
TX Power	Auto
Used SSIDs	Work, Guest-Access

Radio2

Band	5 GHz
Wireless Mode	802.11 AC/N
Preferred Channel	Auto
Channel HT Mode	40 MHz
Extension Channel	Upper Channel
Rate	Auto
TX Power	Auto
Used SSIDs	Work

3. FireCluster

3.1 General

Firecluster Properties

Mode	Active/Passive
Cluster ID	50

Interfaces

Primary FireCluster	Optional-8
Secondary FireCluster	Optional-7
Management	LAN1
Monitored	{WAN1 - Cable} {WAN2 - Fibre} LAN1 DMZ {VLAN Trunk}

3.2 Members

Member Name	Serial Number	Primary Cluster IP	Secondary Cluster IP	Management IP
DataCenter1	V1C504692A55F	169.254.0.1/30	169.254.1.1/30	10.0.1.2/24
DataCenter2	V1C504691A41F	169.254.0.2/30	169.254.1.2/30	10.0.1.3/24

3.3 Advanced

Advanced

Logging and notification	
Lost heartbeat threshold	3
Monitor hardware status	disabled

4. Service Configuration

Order	Action	Name	From	To	Log	Alarm
1	Allow/Proxy	FTP-proxy_Outgoing	LAN1 VOIP	{WAN1 - Cable} {WAN2 - Fibre}	Yes	No
2	Allow/Proxy	SMTP-proxy-SNAT_WAN2_D...	{WAN2 - Fibre}	(Static NAT)	No	No
3	Allow/Proxy	SMTP-proxy-DMZ_WAN2	Email-Server		No	No
4	Allow/Proxy	HTTP-proxy-SNAT_WAN1_D...	{WAN1 - Cable}	(Server Load Balancing)	No	No
5	Allow/Proxy	HTTP-proxy-SNAT_WAN2_D...	{WAN2 - Fibre}	(Server Load Balancing)	No	No
6	Allow/Proxy	HTTP-proxy_Outgoing_non_...	LAN1	{WAN1 - Cable} {WAN2 - Fibre}	Yes	No
7	Allow/Proxy	HTTP-proxy_Outgoing	DMZ VLAN40 VLAN50 VLAN80 surf_users	{WAN1 - Cable} {WAN2 - Fibre}	No	No
8	Allow/Proxy	POP3-proxy_Outgoing	LAN1	{WAN1 - Cable}	No	No
9	Allow/Proxy	HTTPS-proxy_Outgoing	LAN1 DMZ VLAN40 VLAN50 VLAN80	{WAN1 - Cable} {WAN2 - Fibre}	No	No
10	Allow	WatchGuard SSLVPN	Any-External Any-Trusted Any-Optional	Firebox	No	No
11	Allow	WatchGuard Gateway Wireless Controller	Any-Trusted Any-Optional	Firebox	No	No
12	Allow	RDP_Outgoing	LAN1 VLAN40 VLAN50 VLAN80	{WAN1 - Cable}	No	No
13	Allow	WatchGuard Authentication	Any-Trusted Any-Optional	Firebox	No	No
14	Allow	WatchGuard Certificate Portal_Outgoing	LAN1 DMZ VLAN40 VLAN50 VLAN80	Firebox	No	No
15	Allow	WatchGuard Web UI_LAN1_Firebox	LAN1	Firebox	No	No
16	Allow	Ping_Outgoing	LAN1 VOIP DMZ {VLAN1 MGMT} VLAN40 VLAN50 VLAN80 AccessPoints	Any	No	No
17	Allow/Proxy	DNS-proxy_SNAT_WAN1_DMZ	{WAN1 - Cable}	(Static NAT)	No	No
18	Allow/Proxy	DNS-proxy_SNAT_WAN2_DMZ	{WAN2 - Fibre}	(Static NAT)	No	No
19	Allow/Proxy	DNS-proxy_DMZ_WAN2	DNS-Server	{WAN2 - Fibre}	No	No
20	Allow	WatchGuard_LAN1_Firebox	LAN1	Firebox	No	No
21	Allow	TCP-UDP_VLAN	VLAN40 VLAN50	VLAN80	No	No
22	Allow	TCP-UDP_Outgoing	LAN1	Any-Trusted VOIP DMZ {VLAN1 MGMT} VLAN40 VLAN50 VLAN80	No	No
23	Allow	BOVPN-Allow.out	Any	Remote_P2 Remote2	No	No
24	Allow	Allow Hotspot-Users	VLAN80	Any-External	No	No
25	Allow	Allow SSLVPN-Users	SSLVPN-Users@SSL-VPN	Any	No	No
26	Allow	BOVPN-Allow.in	Remote_P2 Remote2	Any	No	No

4.1  FTP-proxy_Outgoing

Policy added on 2016-12-19T14:39:05+01:00.

Policy

Action	From	To
Allow/Proxy	LAN1 VOIP	{WAN1 - Cable} {WAN2 - Fibre}

Properties

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

Miscellaneous & Advanced

Function	
Policy-based routing	Interfaces: {WAN1 - Cable} {WAN2 - Fibre} (Failover Mode)
IPS	enabled
Logging	Log
Schedule	Always On
Traffic Management	Forward: Limit_1Mb, Reverse: default
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)

4.2  SMTP-proxy-SNAT_WAN2_DMZ

Policy added on 2016-12-19T14:15:32+01:00.

Policy

Action	From	To
Allow/Proxy	{WAN2 - Fibre}	Mail-Server_WAN2.snat

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
SMTP-proxy (Proxy: SMTP-Incoming.Standard.Mail-Server)	TCP	25	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)
Tags	Email, SNAT

4.3  SMTP-proxy-DMZ_WAN2

Policy added on 2016-12-19T14:17:24+01:00.

Policy

Action	From	To
Allow/Proxy	Email-Server	{WAN2 - Fibre}

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
SMTP-proxy (Proxy: SMTP-Incoming.Standard.1)	TCP	25	-

Miscellaneous & Advanced

Function	
Policy-based routing	Interface: WAN2 - Fibre
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (for all traffic in this policy with source IP 43.14.57.145)
Tags	Email

4.4  HTTP-proxy-SNAT_WAN1_DMZ

Policy added on 2016-12-19T13:50:40+01:00.

Policy

Action	From	To
Allow/Proxy	{WAN1 - Cable}	Web-Server_WAN1_Cluster.snat

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
HTTP-proxy (Proxy: HTTP-Server.Standard.Web-Server)	TCP	80	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)
Tags	DNS, SNAT

4.5  HTTP-proxy-SNAT_WAN2_DMZ

Policy added on 2016-12-19T14:11:12+01:00.

Policy

Action	From	To
Allow/Proxy	{WAN2 - Fibre}	Web-Server_WAN2-Cluster.snat

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
HTTP-proxy (Proxy: HTTP-Server.Standard.Web-Server.1)	TCP	80	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)
Tags	DNS, SNAT

4.6  HTTP-proxy_Outgoing_non_working_hours

Policy added on 2016-12-19T14:51:58+01:00.

Policy

Action	From	To
Allow/Proxy	LAN1	{WAN1 - Cable} {WAN2 - Fibre}

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
HTTP-proxy (Proxy: HTTP-Client.Standard)	TCP	80	-

Miscellaneous & Advanced

Function	
Policy-based routing	Interfaces: {WAN2 - Fibre} {WAN1 - Cable} (Failover Mode)
IPS	enabled
Logging	Log
Schedule	Non Working Hours
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)

4.7  HTTP-proxy_Outgoing

Policy added on 2016-12-19T14:26:53+01:00.

Policy

Action	From	To
Allow/Proxy	DMZ VLAN40 VLAN50 VLAN80 surf_users	{WAN1 - Cable} {WAN2 - Fibre}

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
HTTP-proxy (Proxy: HTTP-Client.Standard.Outgoing.1)	TCP	80	-

Miscellaneous & Advanced

Function	
Policy-based routing	Interfaces: {WAN2 - Fibre} {WAN1 - Cable} (Failover Mode)
Application Control	Global
IPS	enabled
Bandwidth and Time Quotas	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)
Tags	Web

4.8  POP3-proxy_Outgoing

Policy added on 2016-12-19T14:40:25+01:00.

Policy

Action	From	To
Allow/Proxy	LAN1	{WAN1 - Cable}

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
POP3-proxy (Proxy: POP3-Client.Standard.1)	TCP	110	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)
Tags	Email

4.9  HTTPS-proxy_Outgoing

Policy added on 2016-12-19T14:34:52+01:00.

Policy

Action	From	To
Allow/Proxy	LAN1 DMZ VLAN40 VLAN50 VLAN80	{WAN1 - Cable} {WAN2 - Fibre}

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
HTTPS-proxy (Proxy: HTTPS-Client.Standard.Outgoing)	TCP	443	-

Miscellaneous & Advanced

Function	
Policy-based routing	Interfaces: {WAN2 - Fibre} {WAN1 - Cable} (Failover Mode)
Application Control	Global
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)
Tags	Web

4.10 WatchGuard SSLVPN

Policy added on 2016-12-19T14:50:24+01:00.

Policy

Action	From	To
Allow	Any-External Any-Trusted Any-Optional	Firebox

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
SSL-VPN	TCP	443	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting

4.11 WatchGuard Gateway Wireless Controller

Policy added on 2016-12-19T15:01:21+01:00.

Policy

Action	From	To
Allow	Any-Trusted Any-Optional	Firebox

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
WG-Gateway-Wireless-Controller	UDP	2529	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting

4.12 RDP_Outgoing

Policy added on 2016-12-19T14:41:21+01:00.

Policy

Action	From	To
Allow	LAN1 VLAN40 VLAN50 VLAN80	{WAN1 - Cable}

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
RDP	TCP	3389	-

Miscellaneous & Advanced

Function	
Policy-based routing	Interface: WAN1 - Cable
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)

4.13  WatchGuard Authentication

Policy added on 2016-12-19T14:57:28+01:00.

Policy

Action	From	To
Allow	Any-Trusted Any-Optional	Firebox

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
WG-Auth	TCP	4100	-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use Dynamic NAT (Use global table)

4.14 WatchGuard Certificate Portal_Outgoing

Policy added on 2016-12-19T14:35:49+01:00.

Policy

Action	From	To
Allow	LAN1 DMZ VLAN40 VLAN50 VLAN80	Firebox

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
WG-Cert-Portal	TCP	4126	-

Miscellaneous & Advanced

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

4.15 WatchGuard Web UI_LAN1_Firebox

Policy added on 2016-12-15T09:52:26+01:00.

Policy

Action	From	To
Allow	LAN1	Firebox

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
WG-Fireware-XTM-WebUI	TCP	8080	-

Miscellaneous & Advanced

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

4.16  Ping_Outgoing

Policy added on 2016-12-15T09:52:26+01:00.

Policy

Action	From	To
Allow	LAN1 VOIP DMZ {VLAN1 MGMT} VLAN40 VLAN50 VLAN80 AccessPoints	Any

Properties

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

Miscellaneous & Advanced

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

4.17  DNS-proxy_SNAT_WAN1_DMZ

Policy added on 2016-12-19T13:49:06+01:00.

Policy

Action	From	To
Allow/Proxy	{WAN1 - Cable}	DNS_Server_WAN1.snat

Properties

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

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table)
	Use Dynamic NAT (Use global table)
Tags	DNS, SNAT

4.18  DNS-proxy_SNAT_WAN2_DMZ

Policy added on 2016-12-19T13:47:26+01:00.

Policy

Action	From	To
Allow/Proxy	{WAN2 - Fibre}	DNS_Server_WAN2.snat

Properties

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

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table)
	Use Dynamic NAT (Use global table)
Tags	DNS, SNAT

4.19  DNS-proxy_DMZ_WAN2

Policy added on 2016-12-19T14:19:44+01:00.

Policy

Action	From	To
Allow/Proxy	DNS-Server	{WAN2 - Fibre}

Properties

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

Miscellaneous & Advanced

Function	
Policy-based routing	Interfaces: {WAN2 - Fibre} {WAN1 - Cable} (Failover Mode)
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table)
	Use Dynamic NAT (Use global table)
Tags	DNS

4.20 WatchGuard_LAN1_Firebox

Policy added on 2016-12-15T09:52:26+01:00.

Policy

Action	From	To
Allow	LAN1	Firebox

Properties

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

Miscellaneous & Advanced

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

4.21 TCP-UDP_VLAN

Policy added on 2016-12-19T14:42:03+01:00.

Policy

Action	From	To
Allow	VLAN40 VLAN50	VLAN80

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
TCP-UDP	TCP	0	-
	UDP	0	

Miscellaneous & Advanced

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

4.22 TCP-UDP_Outgoing

Policy added on 2016-12-19T14:42:28+01:00.

Policy

Action	From	To
Allow	LAN1	Any-Trusted VOIP DMZ {VLAN1 MGMT} VLAN40 VLAN50 VLAN80

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
TCP-UDP	TCP	0	-
	UDP	0	

Miscellaneous & Advanced

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

4.23  BOVPN-Allow.out

Policy added on 2016-12-19T14:49:58+01:00.

Policy

Action	From	To
Allow	Any	Remote_P2 Remote2

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Any	Any		-

Miscellaneous & Advanced

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

4.24  Allow Hotspot-Users

Policy added on 2016-12-19T15:04:54+01:00.

Policy

Action	From	To
Allow	VLAN80	Any-External

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Any	Any		-

Miscellaneous & Advanced

Function	
Policy-based routing	Interface: WAN1 - Cable
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting
NAT Rules	Use 1-to-1-NAT (Use global table) Use Dynamic NAT (Use global table)

4.25  Allow SSLVPN-Users

Policy added on 2016-12-19T14:50:24+01:00.

Policy

Action	From	To
Allow	SSLVPN-Users@SSL-VPN	Any

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Any	Any		-

Miscellaneous & Advanced

Function	
IPS	enabled
Schedule	Always On
ICMP Error Handling	Use global setting

4.26  BOVPN-Allow.in

Policy added on 2016-12-19T14:49:58+01:00.

Policy

Action	From	To
Allow	Remote_P2 Remote2	Any

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Any	Any		-

Miscellaneous & Advanced

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

5. Virtual Private Network

5.1 Branch Office VPN

5.1.1 Branch Office Gateways

Local Gateway	Local ID	Local IF	Remote Gateway IP	Remote ID
Remote2 (Virt. IF)	IP address: 43.14.57.144	WAN2 - Fibre	IP Address: 54.23.78.90	IP address: 54.23.78.90

Remote Endpoint Type	Firebox	
Credential Method	Pre-Shared Key	
Phase 1	Mode	Main
	IKE Keep Alive	disabled
	NAT Traversal	Keep-alive interval: 20 seconds; Source Port 4500; Dest. Port: 4500
	Dead Peer Detection	Traffic based, Idle timeout: 20 seconds, Max retries: 5
Phase1 Transform	Auth./Encr. Alg. / Key-Group / SA Lifetime	SHA-1/3DES / Diffie-Hellman Group 2 / 8 hour
		SHA-2(512)/AES(256-bit) / Diffie-Hellman Group 2 / 8 hour

Local Gateway	Local ID	Local IF	Remote Gateway IP	Remote ID
Remote_P1	IP address: 43.14.57.144	WAN2 - Fibre	IP Address: 254.35.123.4	IP address: 254.35.123.4

Credential Method	Pre-Shared Key	
Phase 1	Mode	Main
	IKE Keep Alive	disabled
	NAT Traversal	Keep-alive interval: 20 seconds; Source Port 4500; Dest. Port: 4500
	Dead Peer Detection	Traffic based, Idle timeout: 20 seconds, Max retries: 5
Phase1 Transform	Auth./Encr. Alg. / Key-Group / SA Lifetime	SHA-2(512)/AES(256-bit) / Diffie-Hellman Group 2 / 8 hour
		SHA-2(512)/AES(192-bit) / Diffie-Hellman Group 2 / 8 hour
Auto-Start	enabled	

5.1.2 Branch Office Tunnels

Tunnelname	Gateway	Addresses		
IPSEC-Users		10.0.4.0/24	<==>	192.168.11.10-192.168.11.20

Phase2 Settings	PFS is enabled with DH Group 1
IPSec Proposal	IPSEC-Users_mu (ESP with SHA-1 - AES (256-bit), Key Expiration: 8 hour - 128000 KBytes)

Tunnelname	Gateway	Addresses		
Remote_P2	Remote_P1	10.0.1.0/24 => 10.0.1.5 (DNAT)	==>	192.168.37.0/24

Phase2 Settings	PFS is disabled
IPSec Proposal	ESP-AES-SHA1 (ESP with SHA-1 - AES (256-bit), Key Expiration: 8 hour)

Tunnelname	Gateway	Addresses		
Remote2	Remote2 (Virt. IF)	Any	<==>	Any

Phase2 Settings	PFS is enabled with DH Group 2
IPSec Proposal	ESP-AES-SHA1 (ESP with SHA-1 - AES (256-bit), Key Expiration: 8 hour)
VPN Routes	172.23.0.0/24(Metric:10)

5.2 Mobile User VPN

5.2.1 IPSec

Advanced Settings

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

5.2.1.1 Overview

Order	Action	Name	Type	Log	Alarm	MUVPN Group	Allowed Ressources
1	Allow	IPSEC-Users-Any	Any	No	No	IPSEC-Users	10.0.4.0/24

5.2.1.1.1  IPSEC-Users-Any

Policy added on 2017-05-24T09:09:26+02:00.

Properties

Policy Type	Protocol	Server-Port	Custom Idle Timeout
Any	Any		-

Policy

Disposition	Allowed Resources	Logging
Allow	10.0.4.0/24	

Miscellaneous & Advanced

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

5.2.1.2 IPSec Configuration

5.2.1.2.1 IPSEC-Users

Settings

General Settings	Authentication Server	Firebox-DB
	Passphrase	XXXXXXXX
	Primary / Backup Firebox IP	194.86.213.45 /

IPSec Tunnel

Authentication Method	Use password of end-user profile as Pre-shared key
Phase1 Settings	SHA-1 - 3DES
	SA Life: 8 hour - Key Group: Diffie-Hellman Group 1
	NAT Traversal: Keep-alive interval: 20 seconds (Source Port 4500, Dest. Port: 4500)
	IKE Keep Alive: disabled
Phase2 Settings	SHA-1 - AES (256-bit)
	Key Expiration: 8 hour - 128000 KBytes
	PFS: Diffie-Hellman Group 1

Resources

Allowed Resources	10.0.4.0/24
Virtual IP Address Pool	192.168.11.10-192.168.11.20

Advanced

Connection Mode	Manual
Inactivity timeout	never times out

5.2.2 SSLVPN

General

Primary FB IP address	194.86.213.45
Backup FB IP address	43.14.57.144
Routed VPN Traffic	
Allowed Ressources	10.0.1.0/32, 10.0.4.0/32
IP Address Pool	192.168.113.0/24

Authentication

Authentication Server	Firebox-DB
Auto reconnect after connection lost	enabled
Force users to authenticate	disabled
Allow client to remember password	disabled
Users and Groups	SSLVPN-Users (group)

Advanced

Authentication	SHA-1
Encryption	AES-256
Data Channel	TCP/443
Keep Alive Interval / Timeout	10 seconds / 60 seconds
Renegotiate Data Channel	61 min
Domain Name	
DNS Servers	
WINS Servers	

5.3 VPN Settings

VPN Settings

Add policy to enable outbound IPSec pass-through	disabled
Enable TOS for IPSec	disabled
Enable the use for non-default routes	disabled
Build-in IPSec policy	enabled
Remove VPN routes when tunnel for a BOVPN virtual IF is down	disabled
Enable LDAP server for certificate verification	disabled
BOVPN Notification	

6. Subscription Services

6.1 Update Server

Update Server

Automatic Update	Enabled - Interval: 1 hours
IPS / Application Signatures	enabled
GAV Signatures	enabled
DLP Signatures	enabled
Botnet Detection Sites	enabled
Geolocation Database	enabled
Update Server	https://services.watchguard.com

6.2 spamBlocker

General Settings

Virus Outbread Detection	enabled
VOD maximum file size to scan	100 kilobytes
Max number of connections	32
Max file size to scan	100 Kbytes
Cache size	10000 Entries
Proactive patterns	enabled

Trusted Email Forwarders

	.forwarder.com

Spam Thresholds

Confirmed spam threshold	90
Suspected spam threshold	80

6.3 Gateway AntiVirus

Decompress archives:	Up to 3 levels

6.4 Intrusion Prevention

Scan Mode: Full Scan

Level	Action	Alarm	Log
critical	Drop	disabled	enabled
high	Drop	disabled	enabled
medium	Drop	disabled	enabled
low	Drop	disabled	enabled
info	Allow	disabled	disabled

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

6.5 Reputation Enabled Defense

Policy Name	Proxy Type	Type	RED - block bad reputation URLs	RED - bypass good reputation URLs
HTTP-proxy-SNAT_WAN1_DMZ	HTTP	Firewall	disabled	disabled
HTTP-proxy-SNAT_WAN2_DMZ	HTTP	Firewall	disabled	disabled
HTTP-proxy_Outgoing_non_working_hours	HTTP	Firewall	disabled	disabled
HTTP-proxy_Outgoing	HTTP	Firewall	disabled	disabled

Additional Settings	
Send encrypted scan results to WatchGuard	disabled

6.6 Botnet Detection

Botnet Detection	enabled (Block traffic from suspected botnet sites)

6.7 Geolocation

Geolocation	enabled
Blocked Countries	AFG, ARM, AZE, BHR, BGD, BTN, IOT, BRN, KHM, CHN, CXR, CCK, GEO, JOR, HKG, IND, IDN, IRN, IRQ, ISR, JPN, KAZ, KWT, KGZ, LAO, LBN, MAC, MYS, MDV, MNG, MMR, NPL, PRK, OMN, PAK, PSE, PHL, QAT, KOR, SAU, SGP, LKA, SYR, TWN, TJK, THA, TUR, TKM, ARE, UZB, VNM, YEM

6.8 Data Loss Prevention

6.8.1 Sensors

6.8.1.1 HIPAA Audit Sensor

Type: Build-in
Description: Default HIPAA Audit Sensor; detects and logs attempts to send or receive healthcare-related information

Rules

SocialsecuritynumberswithqualifyingtermsUSA
CreditordebitcardnumberswithqualifyingtermsGlobal
NPI
MedicalPatientFormsUSA
phi
DEANumber

Actions	Source	Destination	Action	Mail Action	Alarm	Log
enabled	Any	Any	allow	allow	enabled	enabled

Settings	in email traffic	in non-email traffic	Alarm	Log
When content exceeds scan limit	allow	allow	enabled	enabled
When a scan error occurs	allow	allow	enabled	enabled
When password protected	allow	allow	enabled	enabled
Limit file scanning to first	5120 kbytes			

6.8.1.2 PCI Audit Sensor

Type: Build-in
Description: Default Payment Card Industry (PCI) Audit Sensor; detects and logs attempts to send or receive credit card information

Rules

CreditordebitcardnumbersGlobal
CCMagStripeTrack1
CCMagStripeTrack2

Actions	Source	Destination	Action	Mail Action	Alarm	Log
enabled	Any	Any	allow	allow	enabled	enabled

Settings	in email traffic	in non-email traffic	Alarm	Log
When content exceeds scan limit	allow	allow	enabled	enabled
When a scan error occurs	allow	allow	enabled	enabled
When password protected	allow	allow	enabled	enabled
Limit file scanning to first	5120 kbytes			

6.8.2 Policies

Policy Name	Sensor

6.8.3 Notification Settings

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	disabled

6.9 APT Blocker

Level	Action	Alarm	Log
High	Drop	disabled	enabled
Medium	Drop	disabled	enabled
Low	Drop	disabled	enabled
Clean	(Allow)		disabled

Policy Name	Proxy Type	APT
FTP-Client.Standard.Outgoing	ftp	enabled
HTTP-Client.Standard.Outgoi...	http	enabled
HTTP-Server.Standard.Web-...	http	enabled
HTTP-Server.Standard.Web-...	http	enabled
POP3-Client.Standard.1	-	disabled
SMTP-Incoming.Standard.1	smtp	enabled
SMTP-Incoming.Standard.M...	smtp	enabled

Alarm Configuration	Parameter
Send SNMP trap	disabled
Send notification	Email (every 15 min or 10 times)