Fortinet Configuration Report

Hostname: "FG3600-Internet"

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

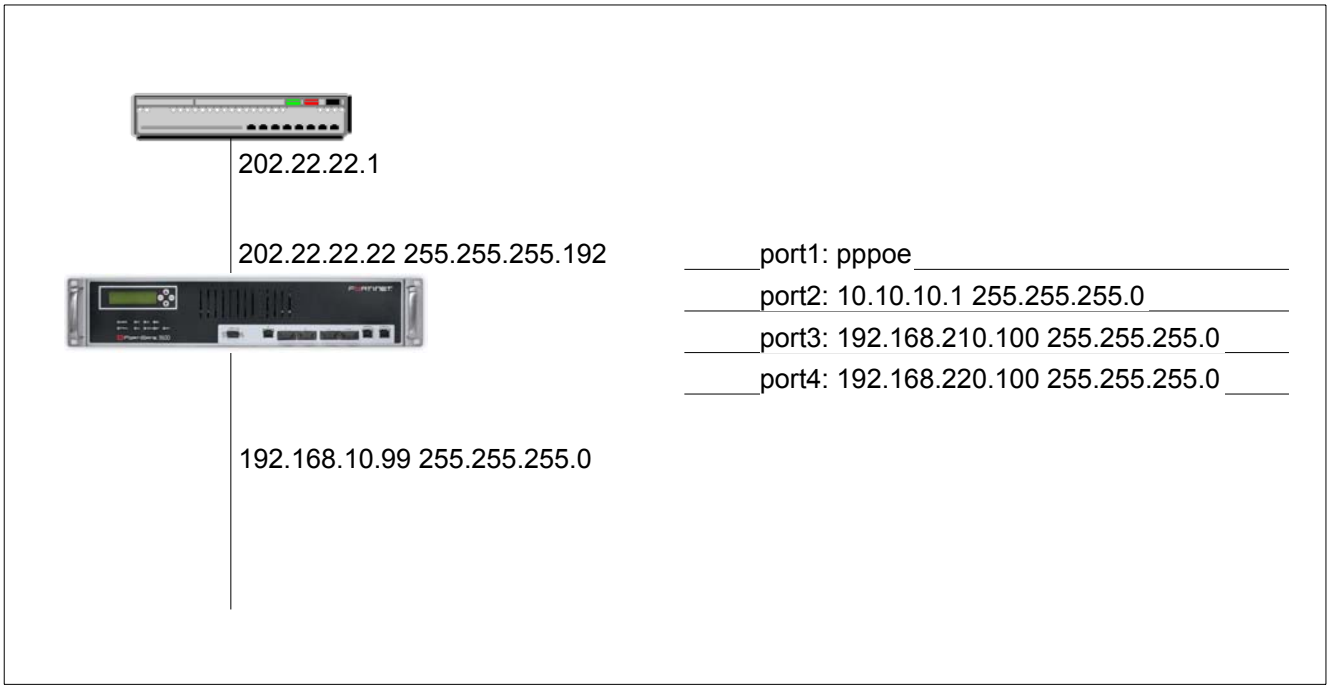
FortiGate FG3600

Firmware Version 2.80 build489 build date 051027

Report printed on SCSY-2 at 11/28/05 18:09:22 with autoDOC Version 6.10

1. System Configuration

Fortigate is configured in Route/NAT mode.



1.1 Status

Paramater	Key
Host Name	FG3600-Internet
Operation Mode	Route/NAT

1.2 Network

1.2.1 Interface

Name	IP - Netmask	Access	Ping Server	MTU	Log
external	202.22.22.22 255.255.255.192		202.11.11.11		enable
internal	192.168.10.99 255.255.255.0	ping https ssh			
port1	pppoe	ping	80.11.11.11		enable
port2	10.10.10.1 255.255.255.0	ping			
port3	192.168.210.100 255.255.255.0				
port4	192.168.220.100 255.255.255.0				

1.2.1.1 Konfiguration auf Interface "port1"

Adressing Mode	PPPoE
User	user@testisp.ch
Unnumbered IP	
Initial Disc Timeout	1
Initial PADT Timeout	1
Distance	20
Retrieve default gateway from server	enable
Override internal DNS	
Connect to Server	enable

1.2.2 DNS

DNS Server	IP
Primary	195.186.1.121
Secondary	195.186.4.121

1.3 DHCP

1.3.1 Service

Interface	Service		
external	NONE		
internal	DHCP Server		
		Name	"internal_dhcp_server"
		Domain	
		Default Gateway	192.168.10.99
		IP Range / Network Mask	192.168.10.210-192.168.10.220 / 255.255.255.0
		Lease Time	7 days, 0 hours, 0 minutes
		DNS Server	192.168.10.99
		WINS Server	
		Options	
port1	NONE		
port2	NONE		
port3	NONE		
port4	NONE		

1.4 Config

1.4.1 Time

Timezone	Adjust for Daylight Saving Changes
(GMT+01:00) Amsterdam, Berlia, Bern, Rome, Stockholm, Vienna	enable

Set Time	NTP Server	Syn Interval
Synchronize with NTP Server	132.246.168.148	60 min

1.4.2 Options

Parameter	Key
Idle Timeout	20
Auth Timeout	30
Web Administration - Language	english
LCD Panel	enable (XXXXXX)
Dead Gateway Detection	Detection Interval: 5 (seconds) Fail-over Detection: 5 (lost consecutive pings)

1.4.3 Replacement Messages

Mail

virus message	"Dangerous Attachment has been Removed. The file \"%%FILE%%\" has been removed because of a virus. It was infected with the \"%%VIRUS%%\" virus. File quarantined as: \"%%QUARFILENAME%%\"."
file block message	"Potentially Dangerous Attachment Removed. The file \"%%FILE%%\" has been blocked. File quarantined as: \"%%QUARFILENAME%%\"."
oversized file message	"This email has been blocked. The email message is larger than the configured file size limit."
fragmented email	"Fragmented emails are blocked."
virus message (splice mode)	"The file %%FILE%% has been infected with the virus %%VIRUS%% File quarantined as %%QUARFILENAME%%"
file block message (splice mode)	"The file %%FILE%% has been blocked. File quarantined as:
oversized file message (splice mode)	"This message is larger than the configured limit and has been blocked."

HTTP

virus message	"<HTML><BODY> High security alert!!! You are not permitted to download the file \"%%FILE%%\" because it is infected with the virus \"%%VIRUS%%\". URL = http://%%URL%% File quarantined as: %%QUARFILENAME%%. </BODY></HTML>"
file block message	"<HTML> <BODY> High security alert!!! You are not permitted to download the file \"%%FILE%%\". URL = http://%%URL%% </BODY>
oversized file message	"<HTML><BODY> Attention!!! The file \"%%FILE%%\" has been blocked. The file is larger than the configured file size limit. URL = http://%%URL%% </BODY></HTML>"
banned word message	"<HTML><BODY>The page you requested has been blocked because it contains a banned word. URL = http://%%URL%%</BODY></HTML>"
URL block message	"<HTML><BODY>The URL you requested has been blocked. URL = %%URL%%</BODY></HTML>"
client block	"<HTML> <BODY> High security alert!!! You are not permitted to upload the file \"%%FILE%%\". URL = http://%%URL%% </BODY> </HTML>"
client anti-virus	"<HTML><BODY> High security alert!!! You are not permitted to upload the file \"%%FILE%%\" because it is infected with the virus \"%%VIRUS%%\". URL = http://%%URL%% File quarantined as: %%QUARFILENAME%%. </BODY></HTML>"
client filesize	"<HTML><BODY> Attention!!! Your request has been blocked. The request is larger than the configured file size limit. URL = http://%%URL%% </BODY></HTML>"
client banned word	"<HTML><BODY>The page you uploaded has been blocked because it contains a banned word. URL = http://%%URL%%</BODY></HTML>"

FTP

virus message	"Transfer failed. The file %%FILE%% is infected with the virus %%VIRUS%%. File quarantined as %%QUARFILENAME%%."
blocked message	"Transfer failed. You are not permitted to transfer the file \"%%FILE%%\"."
oversized message	"File size limit exceeded."

Alert Mail

test message	
virus message	"Virus/Worm detected: %%VIRUS%% Protocol: %%PROTOCOL%% Source IP: %%SOURCE_IP%% Destination IP: %%DEST_IP%% Email Address From: %%EMAIL_FROM%% Email Address To: %%EMAIL_TO%% "
block message	"File Block Detected: %%FILE%% Protocol: %%PROTOCOL%% Source IP: %%SOURCE_IP%% Destination IP: %%DEST_IP%% Email Address From: %%EMAIL_FROM%% Email Address To: %%EMAIL_TO%% "
intrusion message	"The following intrusion was observed: %%NIDS_EVENT%%."
critical event message	"The following critical firewall event was detected: %%CRITICAL_EVENT%%."
disk full message	"The log disk is Full."

Spam

Email IP	"Mail from this IP address is not allowed and has been blocked."
RBL/ORDBL message	"This message has been blocked because it is from a RBL/ORDBL IP address."
HELO/EHLO domain	"This message has been blocked because the HELO/EHLO domain is invalid"
Email address	"Mail from this email address is not allowed and has been blocked."
Mime header	"This message has been blocked because it contains an invalid header."
Returned email domain	"This message has been blocked because the return email domain is invalid."
Banned word	"This message has been blocked because it contains a banned word."
FortiShield URL block	

Category Block

URL block message	"<html><head><title>Webfilter Violation</title></head><body><table width=\"100%\"><tr><td>%%FORTINET%%</td></tr><tr><td bgcolor=#ff6600 align=\"center\">Web Page Blocked</td></tr></table> You have tried to access a web page which is in violation of your internet usage policy. URL: %%URL%% Category: %%CATEGORY%% To have the rating of this web page re-evaluated please contact your administrator. <hr> Powered by %%SERVICE%%.</body></html>"
HTTP error message	"<html><head><title>%%HTTP_ERR_CODE%% %%HTTP_ERR_DESC%%</title></head><body><table width=\"100%\"><tr><td>%%FORTIGUARD%%</td><td align=\"right\">%%FORTINET%%</td></tr><tr><td bgcolor=#3300cc align=\"center\" colspan=2>%%HTTP_ERR_CODE%% %%HTTP_ERR_DESC%%</td></tr></table> The webserver for %%URL%% reported that an error occurred while trying to access the website. Please click <u>here</u> to return to the previous page. <hr> Powered by %%SERVICE%%.</body></html>"

1.5 Admin

1.5.1 Administrators

Adminstrator	Permission	Trusted Host #1	Trusted Host #2	Trusted Host #3
admin	prof_admin			
monitor	read	192.168.10.0 255.255.255.0		

1.5.2 Access Profile

"prof_admin"	Access Control	Read	Write
	System Configuration	yes	yes
	Log & Report	yes	yes
	Security Policy	yes	yes
	Auth Users	yes	yes
	Admin Users	yes	yes
	FortiProtect Update	yes	yes
	System Shutdown	yes	yes

"read"	Access Control	Read	Write
	System Configuration	yes	
	Log & Report	yes	
	Security Policy	yes	
	Auth Users	yes	
	Admin Users	yes	
	FortiProtect Update	yes	
	System Shutdown	yes	

1.6 Update Center

Paramater	Key
Use override Server Address	No
Allow Push Update	Yes
Scheduled Update	Yes - every - 1:15

2. Router

2.1 Static Routes

#	Destination IP / Mask	Gateway	Device	Distance
1	0.0.0.0 0.0.0.0	202.22.22.1	external	10
2	10.10.11.0 255.255.255.0	10.10.10.250	port2	10
3	10.10.12.0 255.255.255.0	10.10.10.111	port2	10

2.2 RIP

2.2.1 General

Parameter	Value	
RIP Version	1	
Default Metric	1	
Default-information-originate	disable	
RIP Timers	Update 30 (seconds) Timeout 180 (seconds)	Garbage 120 (seconds)
Redistribute	Connected Static	disabled disabled

3. Firewall

3.1 Policy Overview

3.1.1 external -> port2

ID	Source	Destination	Schedule	Service	Action	NAT	Anti-Virus	Log	Status
11	pptp-range	DMZ_All	always	ANY	accept			enable	enable
8	all	VIP_WebServer	always	http	accept		strict		enable
9	all	VIP_SMTP_Serve	always	smtp	accept		strict		enable

3.1.2 internal -> external

ID	Source	Destination	Schedule	Service	Action	NAT	Anti-Virus	Log	Status
14	Internal_Net	FG60_2_LAN	always	ANY	encrypt		scan		enable
15	Internal_Net	MUVPN-1	always	RDP	encrypt				enable
16	Internal_Net	MUVPN-2	always	ANY	encrypt		scan		enable
7	all	all	always	DNS	accept	enable			enable
13	Internal_Net	all	Operational Hours	InternetServic	accept	enable	scan	enable	enable

3.1.3 internal -> port1

ID	Source	Destination	Schedule	Service	Action	NAT	Anti-Virus	Log	Status
12	all	all	always	DNS	accept	enable			enable
4	Internal_Net	all	Operational Hours	InternetServic	accept	enable		enable	enable

3.1.4 internal -> port2

ID	Source	Destination	Schedule	Service	Action	NAT	Anti-Virus	Log	Status
10	Internal_Net	DMZ_All	always	ANY	accept		scan		enable

3.1.5 port2 -> external

ID	Source	Destination	Schedule	Service	Action	NAT	Anti-Virus	Log	Status
17	DMZ_All	all	always	ANY	accept	enable	scan	enable	enable

3.2 Policy Detail

3.2.1 external -> port2

ID 11

Source	pptp-range	Range 192.168.10.110 - 192.168.10.112
Destination	DMZ_All	Address Group: "DMZ_net" "DMZ_11" "DMZ_12"
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	ANY	Predefined Service
Action	accept	
Protection Profile		Not activated
Log	enable	
Authentication	enable	Usergroups: "admin-group"

ID 8

Source	all	Subnet 0.0.0.0 0.0.0.0
Destination	VIP_WebServer	Port Forwarding (VIP): external/202.22.22.35 (tcp/80) -> 10.10.10.10 (tcp/80)
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	http	Predefined Service
Action	accept	
Protection Profile	strict	
Log	disable	

ID 9

Source	all	Subnet 0.0.0.0 0.0.0.0
Destination	VIP_SMTP_Server	Port Forwarding (VIP): external/202.22.22.34 (tcp/25) -> 10.10.10.11 (tcp/25)
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	smtp	Predefined Service
Action	accept	
Protection Profile	strict	
Log	disable	

3.2.2 internal -> external

ID 14

Source	Internal_Net	Subnet 192.168.10.0 255.255.255.0
Destination	FG60_2_LAN	Subnet 192.168.20.0 255.255.255.0
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	ANY	Predefined Service
Action	encrypt	
VPN Tunnel	Tu-Geneve	Allow inbound Allow outbound;
Protection Profile	scan	
Log	disable	

ID 15

Source	Internal_Net	Subnet 192.168.10.0 255.255.255.0
Destination	MUVPN-1	IP 192.168.10.240
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	RDP	Custom Service: TCP / 1-65535:3389-3389
Action	encrypt	
VPN Tunnel	Mobile-T1	Allow inbound Allow outbound;
Protection Profile		Not activated
Log	disable	

ID 16

Source	Internal_Net	Subnet 192.168.10.0 255.255.255.0
Destination	MUVPN-2	IP 192.168.10.241
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	ANY	Predefined Service
Action	encrypt	
VPN Tunnel	Mobile-T2	Allow inbound Allow outbound;
Protection Profile	scan	
Log	disable	

ID 7

Source	all	Subnet 0.0.0.0 0.0.0.0
Destination	all	Subnet 0.0.0.0 0.0.0.0
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	DNS	Predefined Service
Action	accept	
NAT	enable	Dynamic IP Pool: disabled; Fixed Port: disabled
Protection Profile		Not activated
Log	disable	

ID 13

Source	Internal_Net	Subnet 192.168.10.0 255.255.255.0
Destination	all	Subnet 0.0.0.0 0.0.0.0
Schedule	Operational Hours	Recurring Schedule: monday tuesday wednesday thursday friday 08:30 18:00
Service	InternetService	Service Group: "FTP" "HTTP" "HTTPS" "NNTP" "POP3"
Action	accept	
NAT	enable	Dynamic IP Pool: disabled; Fixed Port: disabled
Protection Profile	scan	
Log	enable	

3.2.3 internal -> port1

ID 12

Source	all	Subnet 0.0.0.0 0.0.0.0
Destination	all	Subnet 0.0.0.0 0.0.0.0
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	DNS	Predefined Service
Action	accept	
NAT	enable	Dynamic IP Pool: disabled; Fixed Port: disabled
Protection Profile		Not activated
Log	disable	

ID 4

Source	Internal_Net	Subnet 192.168.10.0 255.255.255.0
Destination	all	Subnet 0.0.0.0 0.0.0.0
Schedule	Operational Hours	Recurring Schedule: monday tuesday wednesday thursday friday 08:30 18:00
Service	InternetService	Service Group: "FTP" "HTTP" "HTTPS" "NNTP" "POP3"
Action	accept	
NAT	enable	Dynamic IP Pool: disabled; Fixed Port: disabled
Protection Profile		Not activated
Log	enable	
Authentication	enable	Usergroups: "admin-group" "user-group"

3.2.4 internal -> port2

ID 10

Source	Internal_Net	Subnet 192.168.10.0 255.255.255.0
Destination	DMZ_All	Address Group: "DMZ_net" "DMZ_11" "DMZ_12"
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	ANY	Predefined Service
Action	accept	
Protection Profile	scan	
Log	disable	

3.2.5 port2 -> external

ID 17

Source	DMZ_All	Address Group: "DMZ_net" "DMZ_11" "DMZ_12"
Destination	all	Subnet 0.0.0.0 0.0.0.0
Schedule	always	Recurring Schedule: sunday monday tuesday wednesday thursday friday saturday
Service	ANY	Predefined Service
Action	accept	
NAT	enable	Dynamic IP Pool: disabled; Fixed Port: disabled
Protection Profile	scan	
Log	enable	

3.3 Addresses & Groups

3.3.1 Address

Adress Name	Type	IP
all	Subnet	0.0.0.0 0.0.0.0
DMZ_11	Subnet	10.10.11.0 255.255.255.0
DMZ_12	Subnet	10.10.12.0 255.255.255.0
DMZ_net	Subnet	10.10.10.0 255.255.255.0
FG60_2_LAN	Subnet	192.168.20.0 255.255.255.0
Internal_Net	Subnet	192.168.10.0 255.255.255.0
MUVPN-1	IP	192.168.10.240
MUVPN-2	IP	192.168.10.241
pptp-range	Range	192.168.10.110 - 192.168.10.112

3.3.2 Address-Groups

Group Name	Member
DMZ_All	"DMZ_net" "DMZ_11" "DMZ_12"

3.4 Services

3.4.1 Custom Services

Service Name	Detail
ICA	TCP / 1-65535 : 1494-1494
Radius-1	UDP / 1-65535 : 1645-1645
Radius-2	UDP / 1-65535 : 1812-1812
RDP	TCP / 1-65535 : 3389-3389

3.4.2 Service Group

Group Name	Members
InternetService	"FTP" "HTTP" "HTTPS" "NNTP" "POP3"
Radius-Services	"Radius-1" "Radius-2"

3.5 Schedule

3.5.1 Recurring Schedules

Name	Day	Start	Stop
always	sunday monday tuesday wednesday thursday friday saturday	00:00	00:00
Operational Hours	monday tuesday wednesday thursday friday	08:30	18:00

3.6 Virtual IP

Name	Type	IP	Service Port	Map to IP	Map to Port
VIP_SMTP_Server	Port Forwarding	external / 202.22.22.34	tcp / 25	10.10.10.11	tcp / 25
VIP_WebServer	Port Forwarding	external / 202.22.22.35	tcp / 80	10.10.10.10	tcp / 80

3.7 Protection Profile

3.7.1 "scan"

Anti-Virus	HTTP	FTP	IMAP	POP3	SMTP
Splice		enable			enable
Virus Scan	enable	enable	enable	enable	enable
File Block					
Pass Fragmented Emails					
Buffer to Disk					
Oversized File/Email	block	block	pass	pass	pass
Add signature to outgoing emails	disable				

Web Filtering	HTTP
Web Content Block	
Web URL Block	
Web Exempt List	
Web Script Filter	
Web Resume Download Block	

Web Category Filtering	HTTP
Enable category block	
Block unrated websites	
Details for blocked HTTP 4xx and 5xx errors	
Rate images by URL	
Allow websites when a rating error occurs	

Spam Filtering	IMAP	POP3	SMTP
IP address FortiGuard - AntiSpam check			
URL FortiGuard - AntiSpam check			
IP address BWL check			
RBL & ORDBL check			
HELO DNS lookup			
E-mail address BWL check			
Return e-mail DNS check			
MIME headers check			
Banned word check			
Spam Action	tag	tag	tag
Append to:	subject	subject	MIME
Append with:	Spam	Spam	Spam:

IPS	Value
IPS Signature	
IPS Anomaly	

Content/Archive Log	HTTP	FTP	IMAP	POP3	SMTP
Display content meta-information on	enable	enable	enable	enable	enable
Archive content meta-information to FortiLog					

3.7.2 "strict"

Anti-Virus	HTTP	FTP	IMAP	POP3	SMTP
Splice		enable			enable
Virus Scan	enable	enable	enable	enable	enable
File Block	enable	enable	enable	enable	enable
Pass Fragmented Emails					
Buffer to Disk					
Oversized File/Email	block	block	block	block	block
Add signature to outgoing emails	disable				

Web Filtering	HTTP
Web Content Block	enable
Web URL Block	enable
Web Exempt List	enable
Web Script Filter	enable
Web Resume Download Block	

Web Category Filtering	HTTP
Enable category block	enable
Block unrated websites	enable
Details for blocked HTTP 4xx and 5xx errors	enable
Rate images by URL	enable
Allow websites when a rating error occurs	enable

Spam Filtering	IMAP	POP3	SMTP
IP address FortiGuard - AntiSpam check			
URL FortiGuard - AntiSpam check			
IP address BWL check			enable
RBL & ORDBL check			enable
HELO DNS lookup			enable
E-mail address BWL check	enable	enable	enable
Return e-mail DNS check	enable	enable	enable
MIME headers check	enable	enable	enable
Banned word check	enable	enable	enable
Spam Action	tag	tag	discard
Append to:	subject	MIME	
Append with:	Spam	Spam: abc	

IPS	Value
IPS Signature	
IPS Anomaly	enable

Content/Archive Log	HTTP	FTP	IMAP	POP3	SMTP
Display content meta-information on	enable	enable	enable	enable	enable
Archive content meta-information to FortiLog					

4. User

4.1 Local User

User Name	Type	Status
admin-user	Local	
user	Local	

4.2 Radius

Name	Server Name/IP
OTP_Server	192.168.10.54

4.3 LDAP

Name	Server Name/IP	Port	Common Name Identifier	Distinguished Name
intern_LDAP	192.168.10.55	389	cn	

4.4 User Group

Group Name	Members	Protection Profile
admin-group	"admin-user"	scan
user-group	"OTP_Server" "intern_LDAP"	strict

5. VPN

5.1 IPSec

5.1.1 Phase 1

Gateway Name	Remote Gateway	Mode	Encr./Auth. Algorithm	Peer Options
Branch_Geneve	Static/30.30.30.30	main	3des-sha1	Accept any peer ID
	P1 Proposal	DH Group	5	
		Keylife	28800	
	XAuth	disable		
	Nat-traversal	enable		
	Keepalive Frequency			
	Dead Peer Detection	enable		
Mobile-U1	Dialup	aggressive	aes256-sha1	Accept this peer ID: "user-1"
	P1 Proposal	DH Group	5	
		Keylife	28800	
	XAuth	Enable as Server	mixed	
		Usergroup:	"user-group"	
	Nat-traversal	enable		
	Keepalive Frequency			
	Dead Peer Detection	enable		
Mobile-U2	Dialup	aggressive	aes192-sha1	Accept this peer ID: "user-2"
	P1 Proposal	DH Group	5	
		Keylife	28800	
	XAuth	Enable as Server	mixed	
		Usergroup:	"user-group"	
	Nat-traversal	enable		
	Keepalive Frequency			
	Dead Peer Detection	enable		

5.1.2 Phase 2

Tunnel Name	Remote Gateway	Encr./Auth. Algorithm		Concentrator
Mobile-T1	"Mobile-U1"	aes256-sha1		
	Enable replay detection	enable		
	Enable perfect forward secrecy(PFS)	enable	DH group: 5	
	Keylife	1800 (Seconds)		
	Autokey Keep Alive	disable		
	Internet browsing	None		
	Quick Mode Identities	Use selectors from policy		
Mobile-T2	"Mobile-U2"	aes256-sha1 aes192-sha1 3des-md5		
	Enable replay detection	enable		
	Enable perfect forward secrecy(PFS)	enable	DH group: 5	
	Keylife	1800 (Seconds)		
	Autokey Keep Alive	disable		
	Internet browsing	None		
	Quick Mode Identities	Use selectors from policy		
Tu-Geneve	"Branch_Geneve"	aes192-sha1 3des-sha1		
	Enable replay detection	enable		
	Enable perfect forward secrecy(PFS)	enable	DH group: 5	
	Keylife	1800 (Seconds)		
	Autokey Keep Alive	disable		
	Internet browsing	None		
	Quick Mode Identities	Use selectors from policy		

5.2 PPTP

Status	Starting IP	Ending IP	User Group
Enable	192.168.10.110	192.168.10.112	admin-group

5.3 L2TP

Status	Starting IP	Ending IP	User Group
Disable			

6. Anti-Virus

6.1 File Block

Pattern	HTTP	FTP	IMAP	POP3	SMTP
*.bat	enable	enable	enable	enable	enable
*.com	enable	enable	enable	enable	enable
*.dll	enable	enable	enable	enable	enable
*.doc					
*.exe	enable	enable	enable	enable	enable
*.gz	enable	enable	enable	enable	enable
*.hta	enable	enable	enable	enable	enable
*.pif	enable	enable	enable	enable	enable
*.ppt			enable	enable	enable
*.rar	enable	enable	enable	enable	enable
*.scr	enable	enable	enable	enable	enable
*.tar	enable	enable	enable	enable	enable
*.tgz	enable	enable	enable	enable	enable
*.vb?	enable	enable	enable	enable	enable
*.wps	enable	enable	enable	enable	enable
*.xl?					
*.zip	enable	enable			

6.2 Config

6.2.1 Oversize Threshold Configuration

Protocol	max. filesize to scan	max. uncompressed size to scan	Ports
HTTP	25 MBs	25 MBs	80
FTP	25 MBs	25 MBs	21
IMAP	25 MBs	25 MBs	143
POP3	25 MBs	25 MBs	110
SMTP	25 MBs	25 MBs	25

6.2.2 Grayware

Category	Status
Adware	enable
BHO	enable
Dial	enable
Download	enable
Game	enable
HackerTool	enable
Hijacker	enable
Joke	enable
Keylog	enable
Misc	enable
NMT	enable
P2P	enable
Plugin	enable
RAT	enable
Spy	enable
Toolbar	enable

7. Web Filter

7.1 Category Block Configuration

Options	Status
FortiGuard Service	enable
Cache	

7.2 Script Filter

Filtering Options	Status
Java Applet	
Cookie	enable
ActiveX	enable

8. Log & Report

8.1 Log Setting

Syslog	**disabled**

WebTrends	**disabled**

Disk	**enabled**
Maximum size of log file:	100 MB
Roll log time	0:0:0 (hh:mm:ss)
Roll Log Frequency	24 hour
Roll log day	sunday
Roll log policy	overwrite
Level	information
Upload When Rolling	disabled

Memory	**disabled**

Fortilog	**enabled**
Name/IP	194.191.86.36
Level	information
Encrypt	
Local ID	

8.2 Log Filter

	Syslog	WebTrends	Disk	Memory	Fortilog	Alert E-mail
Traffic Log			**enable**		**enable**	
Policy allowed traffic			enable		enable	
Policy violation traffic			enable		enable	
Event Log			**enable**		**enable**	
System Activity event			enable		enable	
IPSec negotiation event			enable		enable	
DHCP service event			enable		enable	
L2TP/PPTP/PPPoE service event			enable		enable	
Admin event			enable		enable	
HA activity event			enable		enable	
Firewall authentication event			enable		enable	
Pattern update event			enable		enable	
Anti-virus Log			**enable**		**enable**	
Virus infected			enable		enable	
Filename blocked			enable		enable	
File oversized			enable		enable	
Web Filter Log					**enable**	
Content block					enable	
URL block					enable	
URL exempt					enable	
Blocked category ratings					enable	
Monitored category ratings					enable	
Category rating errors					enable	
Attack Log			**enable**		**enable**	
Attack Signature			enable		enable	
Attack Anomaly			enable		enable	
Spam Filter Log					**enable**	
SMTP					enable	
POP3					enable	
IMAP					enable	