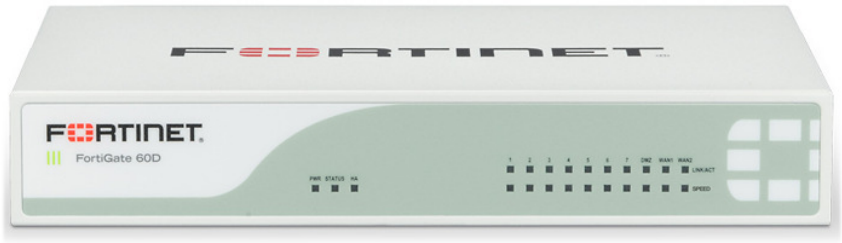
Fortinet Configuration Report

Hostname: FG60D-Web

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



FortiGate FGT60D

Firmware Version 5.6.0 build1449 build date 170330

Report printed on client01 at 05/12/17 10:26:45 with autodoc Version 9.91

Table of Contents

1. Network

Host Name: FG60D-Web

System is running in NAT/Route Mode

System uses flow-based inspection

1.1 Interfaces

Interface	Additional Info	IP / Netmask	Access	Role
Hard-switch				
internal	Member: internal1 internal2 internal3 internal4	192.168.1.99/24	ping https ssh http fgfm capwap	lan
Physical				
dmz		192.168.51.99/24	ping https http fgfm capwap	dmz
internal5		192.168.50.99/24		
internal6		192.168.52.99/24	snmp fgfm radius-acct	
internal7		169.254.1.1/24	ping capwap	
vsw.internal7	VLAN (id:1)	0.0.0.0/0		
VLAN30	VLAN (id:30)	10.10.30.99/24		
VLAN40	VLAN (id:40)	10.10.40.99/24		
wan1		194.191.86.190/26	ping https ssh	wan
Dialup	Tunnel IF			
SitetoSite	Tunnel IF			
wan2		dhcp	ping fgfm	wan
Vap-switch				
guest	SSID: guest	10.10.11.99/24		lan
work	SSID: work	10.10.12.99/24		lan

1.1.1 Additional Configurations on Interfaces

wan2

Adressing Mode: DHCP	Distance/Priority	5/10
	Retrieve default gateway from server	enable
	Override internal DNS	enable

internal7

Adressing Mode	Dedicated to FortiSwitch

internal

Type	Hard-Switch
Member	internal1
	internal2
	internal3
	internal4

guest

Device Management	Device Detection	enable

work

Device Management	Device Detection	enable

1.1.2 DHCP

1.1.2.1 DHCP Server

Interface	Type	IP Range	Network Mask	Def. GW
internal	regular	192.168.1.110-192.168.1.210	255.255.255.0	192.168.1.99
Lease	7 d, 0 h, 0 min			
FC On-Net Status	enable			
DNS Server	Same as System DNS			
Bootstrap Server				
guest	regular	10.10.11.100-10.10.11.254	255.255.255.0	10.10.11.99
Lease	7 d, 0 h, 0 min			
FC On-Net Status	enable			
DNS Server	Same as System DNS			
Bootstrap Server				
work	regular	10.10.12.100-10.10.12.254	255.255.255.0	10.10.12.99
Lease	7 d, 0 h, 0 min			
FC On-Net Status	enable			
DNS Server	Same as System DNS			
Bootstrap Server				
internal7	regular	169.254.1.2-169.254.1.254	255.255.255.0	169.254.1.1
Lease	7 d, 0 h, 0 min			
FC On-Net Status	enable			
DNS Server	-			
Bootstrap Server				
Match VCI	"FortiSwitch" "FortiExtender"			

1.2 DNS

DNS Server	IP
Primary	208.91.112.53
Secondary	208.91.112.52

1.3 Routing

1.3.1 Static Routes

#	Destination Subnet	Device	Gateway	Dist./Prio.	Comment
1	0.0.0.0/0	wan1	194.191.86.129	5/0	
2	192.168.100.0/24	internal5	192.168.50.254	10/0	
3	192.168.101.0/24	internal5	192.168.50.254	10/0	
4	10.10.15.0/24	SitetoSite		10/0	VPN: SitetoSite (Created by VPN wizard)
5	0.0.0.0/0	wan2	1.2.3.4	10/10	

1.3.2 Policy Routes

#	Inc. IF	Source	Destination	Prot./Ports	ToS	-> Action/Gateway (IF)
1	internal6	192.168.51.10/32	0.0.0.0/0	ANY	0x00/0x00	-> 0.0.0.0(wan2)
2	internal6	192.168.51.11/32	0.0.0.0/0	ANY	0x00/0x00	-> 0.0.0.0(wan2)
3	internal6	192.168.51.12/32	0.0.0.0/0	ANY	0x00/0x00	-> 0.0.0.0(wan2)

1.3.3 Router Settings

ECMP Load Balancing Method: Source IP based

1.4 Routing Protokolle

1.4.1 RIP

General	Value
RIP Version	2
Default Metric	1
Default-information-originate	disable
RIP Timers	Update 30 sec.; Timeout 180 sec.; Garbage 120 sec.
Redistribute	connected: disable static: disable ospf: disable bgp: disable

Networks	IP/Mask
1	10.10.50.0 255.255.255.0

Interface	Send Version	Receive Version	Authentication	Passive IF	Split Horizon
wan2	2	2	None	disable	poisoned

1.4.2 OSPF

Parameter	Value
Router ID	192.168.1.99
Default Information	None

Areas	Type	Authentication
0.0.0.0	regular	none

Networks	Area
192.168.1.0 255.255.255.0	0.0.0.0

Name	Interface	Cost	IP	Authentication
Router1-Ext	internal	0	0.0.0.0	none
	Hello Interval	10 seconds		
	Dead Interval	40 seconds		

1.4.3 BGP

Parameter	Value
Local As	65075
Router ID	0.0.0.75
Neighbors	10.127.0.117 - Remote As: 65117

2. System

2.1 Admin

2.1.1 Administrators

Administrator	Permission	Type	Trusted Hosts	VDOM
admin	super_admin	regular		root
monitor	read_only	regular	192.168.1.0/24	root

SMS: Fortiguard Messaging Service, Phone Number: 411112223344
Two-Factor: Fortitoken (FTKMOB3952C93E46)

2.1.2 Admin Profile

prof_admin	Access Control	Rights
	Maintenance	read-write
	Administrator Users	read-write
	FortiGuard Update	read-write
	User & Device	read-write
	System Configuration	read-write
	Network Configuration	read-write
	Log & Report	read-write
	Router Configuration	read-write
	Firewall Configuration	read-write
	VPN Configuration	read-write
	Security Profile Configuration	read-write
	WAN Opt & Cache	read-write
	Endpoint Security	read-write
	WiFi Controller	read-write

read_only	Access Control	Rights
	Maintenance	read
	Administrator Users	read
	FortiGuard Update	read
	User & Device	read
	System Configuration	read
	Network Configuration	read
	Log & Report	read
	Router Configuration	read
	Firewall Configuration	read
	VPN Configuration	read
	Security Profile Configuration	read
	WAN Opt & Cache	read
	Endpoint Security	read
	WiFi Controller	read

2.1.3 Settings

Parameter	Key	Value
Central Management	FortiCloud	fortinet@boll.ch
Administration Settings	HTTP port	80
	Redirect to HTTPS	enable
	HTTPS port	443
	HTTPS Server Certificate	Fortinet_Factory
	Telnet	23
	SSH	22
	Idle Timeout	60 mins
	Allow multiple concurrent sessions for each administrator	enable
CLI Admin Settings	Accepted TLS/SSL versions	tlsv1-1 tlsv1-2
	Lockout Threshold / Duration	3 / 60 min
View Settings	Language	English
	Lines Per Page	50
	Theme	green
	Inspection Mode	flow
	NGFW Mode	profile-based

2.2 Other System Settings

2.2.1 Time

Settings

Timezone	(GMT-08:00) Pacific Time (US&Canada)
Daylight Saving	enable
NTP	enable - Use FortiGuard Servers, Sync Interval: 60 min
NTP Server	enable - Listen on Interfaces: internal7

2.2.2 Replacement Messages

2.2.2.1 Image List

Image Name	Image Type
logo_fnet	gif
logo_fguard_wf	gif
logo_fw_auth	png
logo_v2_fnet	png
logo_v2_fguard_wf	png
logo_v2_fguard_app	png

2.2.3 FortiGuard

AntiVirus and IPS Options

Accept Push Update	No
Scheduled Update	Yes - daily - 2:60 (60 minutes means a random minute)
Improve IPS quality	disable
Use extended IPS signature package	regular

Web Filtering and AntiSpam Options

Webfilter Cache	enabled - TTL: 3600 sec., Timeout: 15 sec.
Anti-Spam Cache	enabled - TTL: 1800 sec., Memory: 2%, Timeout: 7 sec.
FortiGuard Filtering Port	53

2.2.4 Security Fabric

Cooperative Security Fabric CSF

Group name	Fortinet

FortiAnalyzer logging

IP Address	192.168.1.160
Upload Option	realtime
Encrypt Log Transmission	high
Reliability	enable

Sandbox inspection

FortiSandbox Cloud

HTTP Service

Router ID	192.168.1.99
FortiWeb IPs	192.168.1.161 255.255.255.255
Authentication	disable

SMTP Service - FortiMail

Router ID	192.168.1.99
FortiMail IPs	192.168.1.162 255.255.255.255
Authentication	disable

2.2.5 Advanced

FortiClient Endpoint Registration: disable

Email Service

SMTP Server:Port	notification.fortinet.net:465
Default Reply To	
Authentication	disable
Security Mode	smtps

USB Auto-Install	**Key**
Update Fortigate Configuration at restart	Yes - use config file name "fgt_system.conf"
Update Fortigate Firmware at restart	Yes - use image file name "image.out"

2.2.6 Feature Select

Basic Features

Advanced Routing	enable
IPv6	enable
Switch Controller	enable
VPN	enable
WiFi Controller	enable

Security Features

AntiVirus	enable
Application Control	enable
DNS Filter	enable
Endpoint Control	enable
Intrusion Protection	enable
Web Filter	enable

Additional Features

Advanced Endpoint Control	disable
Allow unnamed Policy	enable
Certificates	enable
DNS Database	enable
Domain & IP Reputation	enable
DoS Policy	enable
Email Collection	enable
FortiExtender	disable
ICAP	disable
Implicit Firewall Policies	enable
Load Balance	enable
Local In Policy	enable
Local Reports	disable
Multicast Policy	enable
Multiple Interface Policies	enable
Multiple Security Profiles	enable
NAT46 & NAT64	disable
Policy Learning	enable
Policy-based IPSec VPN	enable
SD-WAN Interface	enable
SSL-VPN Personal Bookmark Management	enable
SSL-VPN Realms	enable
Threat Weight Tracking	enable
Traffic Shaping	enable
VoIP	disable
Wireless Open Security	enable

CLI only Features

AP Profiles	enable
Custom Language	disable
DHCP Advanced Settings	enable
Dynamic Profiles	disable
FortiAP Split Tunneling	disable
IPSec Manual Key	disable
Replacement Message Groups	disable
Webfilter Advanced Settings	disable
Object Colors	disable
Advanced Policy	disable
Display Hostname	disable

2.3 Certificates

Local Certificates

Fortinet_CA_SSL	This is the default CA certificate the SSL Inspection will use when generating new server certificates.
Fortinet_CA_Untrusted	This is the default CA certificate the SSL Inspection will use when generating new server certificates.
Fortinet_SSL	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_RSA1024	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_RSA2048	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_DSA1024	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_DSA2048	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_ECDSA256	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_ECDSA384	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_RSA	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_DSA	This certificate is embedded in the hardware at the factory and is unique to this unit.
Fortinet_SSL_ECDSA	This certificate is embedded in the hardware at the factory and is unique to this unit.

3. Policy & Objects

3.1 Policy

3.1.1 Policy Overview

3.1.1.1 SitetoSite -> internal

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
4	SitetoSite_remote	SitetoSite_local	ALL	ACCEPT		X	

3.1.1.2 guest -> wan1

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
7	guest	all	ALL	ACCEPT	X	X	X

3.1.1.3 internal -> SitetoSite

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
3	SitetoSite_local	SitetoSite_remote	ALL	ACCEPT		X	

3.1.1.4 internal -> internal6

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
2	all	Server	FTP, LDAP, RDP, SSH	ACCEPT		X	X

3.1.1.5 internal -> wan1

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
1	all	all	ALL	ACCEPT		X	X

3.1.1.6 internal5 -> wan1

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
6	all	all	ALL	ACCEPT	X	X	X

3.1.1.7 wan1 -> internal

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
5	all	VIP_svrMail01	ALL	ACCEPT		X	

3.1.1.8 work -> internal

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
9	work	LAN	ALL	ACCEPT		X	

3.1.1.9 work -> wan1

ID	Source/User/Device	Destination	Service	Action	UTM	Log	NAT
8	work	all	ALL	ACCEPT	X	X	X

3.1.2 Policy Detail

3.1.2.1 SitetoSite -> internal

ID 4	vpn_SitetoSite_remote	
Source	SitetoSite_remote	Address Group: SitetoSite_remote_subnet_1
Destination	SitetoSite_local	Address Group: SitetoSite_local_subnet_1
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
Log	enable	Security Events
Log at Session Start	disable	
Capture Packets	disable	
Comments		VPN: SitetoSite (Created by VPN wizard)

3.1.2.2 guest -> wan1

ID 7		
Source	guest	Range: 10.10.11.100 - 10.10.11.254
Destination	all	Subnet: 0.0.0.0/0
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
NAT	enable	Use Outgoing Interface Address
Security Profiles	AntiVirus	default
	Proxy Options	default
	SSL/SSH Inspection	certificate-inspection
Log	enable	Security Events
Log at Session Start	disable	
Capture Packets	disable	

3.1.2.3 internal -> SitetoSite

ID 3	vpn_SitetoSite_local	
Source	SitetoSite_local	Address Group: SitetoSite_local_subnet_1
Destination	SitetoSite_remote	Address Group: SitetoSite_remote_subnet_1
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
Log	enable	Security Events
Log at Session Start	disable	
Capture Packets	disable	
Comments		VPN: SitetoSite (Created by VPN wizard)

3.1.2.4 internal -> internal6

ID 2	ServerAccess	
Source	all	Subnet: 0.0.0.0/0
Destination	Server	Address Group: "svrDC01" "svrRAD01"
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	FTP	TCP: 21
	LDAP	TCP: 389
	RDP	TCP: 3389
	SSH	TCP: 22
Action	accept	
NAT	enable	Use Outgoing Interface Address
Log	enable	All Sessions
Log at Session Start	disable	
Capture Packets	disable	

3.1.2.5 internal -> wan1

ID 1	WebTraffic	
Source	all	Subnet: 0.0.0.0/0
Destination	all	Subnet: 0.0.0.0/0
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
NAT	enable	Use Outgoing Interface Address
Log	enable	All Sessions
Log at Session Start	disable	
Capture Packets	disable	

3.1.2.6 internal5 -> wan1

ID 6		
Source	all	Subnet: 0.0.0.0/0
Destination	all	Subnet: 0.0.0.0/0
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
NAT	enable	Use Outgoing Interface Address
Security Profiles	AntiVirus	default
	Web Filter	default
	Proxy Options	default
	SSL/SSH Inspection	certificate-inspection
Log	enable	All Sessions
Log at Session Start	disable	
Capture Packets	disable	

3.1.2.7 wan1 -> internal

ID 5	OWA	
Source	all	Subnet: 0.0.0.0/0
Destination	VIP_svrMail01	Port Forwarding (VIP): wan1/194.191.86.190 (tcp/4000) -> 192.168.1.210 (tcp/4000)
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
Log	enable	All Sessions
Log at Session Start	disable	
Capture Packets	disable	

3.1.2.8 work -> internal

ID 9		
Source	work	Range: 10.10.12.100 - 10.10.12.254
Destination	LAN	Subnet: 192.168.1.0/24
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
Log	enable	Security Events
Log at Session Start	disable	
Capture Packets	disable	

3.1.2.9 work -> wan1

ID 8		
Source	work	Range: 10.10.12.100 - 10.10.12.254
Destination	all	Subnet: 0.0.0.0/0
Schedule	always	Recurring: sunday monday tuesday wednesday thursday friday saturday, 0:00 - 0:00
Service	ALL	IP: 0
Action	accept	
NAT	enable	Use Outgoing Interface Address
Security Profiles	AntiVirus	default
	Web Filter	default
	Proxy Options	default
	SSL/SSH Inspection	certificate-inspection
Log	enable	Security Events
Log at Session Start	disable	
Capture Packets	disable	

3.1.3 Specific Log Settings

Log Setting	
Log implicit denied traffic (Policy ID 0)	disable

3.2 Firewall Objects

3.2.1 Address

3.2.1.1 Address

Type	Address Name	Value	Interface
IP			
	FortiAnalyzer	192.168.1.160	internal
	FortiMail	192.168.1.162	internal
	FortiWeb	192.168.1.161	internal
	none	0.0.0.0	
	svrDC01	192.168.52.205	internal6
	svrMail01	192.168.205.210	internal6
	svrRAD01	192.168.52.200	internal6
SUBNET			
	DMZ	192.168.51.0/24	dmz
	FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0	
	LAN	192.168.1.0/24	internal
	SitetoSite_local_subnet_1	192.168.1.0/24	
	SitetoSite_remote_subnet_1	10.10.15.0/24	
	VoIP	192.168.50.0/24	internal5
	all	0.0.0.0/0	
IPRANGE			
	SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	ssl.root(SSL VPN interface)
	guest	10.10.11.100 - 10.10.11.254	guest
	work	10.10.12.100 - 10.10.12.254	work
FQDN			
	auth.gfx.ms	auth.gfx.ms	
	autoupdate.opera.com	autoupdate.opera.com	
	google-play	play.google.com	
	softwareupdate.vmware.com	softwareupdate.vmware.com	
	swscan.apple.com	swscan.apple.com	
	update.microsoft.com	update.microsoft.com	
WILDCARD-FQDN			
	Adobe Login	*.adobelogin.com	
	Gotomeeting	*.gotomeeting.com	
	Windows update 2	*.windowsupdate.com	
	adobe	*.adobe.com	
	android	*.android.com	
	apple	*.apple.com	
	appstore	*.appstore.com	
	citrix	*.citrixonline.com	
	dropbox.com	*.dropbox.com	
	eease	*.eease.com	
	firefox update server	aus*.mozilla.org	
	fortinet	*.fortinet.com	
	google-drive	*drive.google.com	
	google-play2	*.ggpht.com	
	google-play3	*.books.google.com	
	googleapis.com	*.googleapis.com	
	icloud	*.icloud.com	
	itunes	*itunes.apple.com	
	live.com	*.live.com	
	microsoft	*.microsoft.com	
	skype	*.messenger.live.com	
	verisign	*.verisign.com	
MULTICAST			
	Bonjour	224.0.0.251 - 224.0.0.251	
	EIGRP	224.0.0.10 - 224.0.0.10	
	OSPF	224.0.0.5 - 224.0.0.6	
	all	224.0.0.0 - 239.255.255.255	
	all_hosts	224.0.0.1 - 224.0.0.1	
	all_routers	224.0.0.2 - 224.0.0.2	

3.2.1.2 Group

Group Name	Member
Dialup_split	all
Fortinet	FortiAnalyzer, FortiMail, FortiWeb
Server	svrDC01, svrRAD01
SitetoSite_local	SitetoSite_local_subnet_1
SitetoSite_remote	SitetoSite_remote_subnet_1

3.2.2 Service

3.2.2.1 Service

Service Name	Protocol	IP/FQDN	Visibility
GENERAL			
ALL	IP: ANY		
ALL_ICMP	ICMP (:ANY)		
ALL_ICMP6	ICMP6 (:ANY)		
ALL_TCP	TCP: 1-65535		
ALL_UDP	UDP: 1-65535		
WEB ACCESS			
HTTP	TCP: 80		
HTTPS	TCP: 443		
FILE ACCESS			
AFS3	TCP: 7000-7009, UDP: 7000-7009		
FTP	TCP: 21		
FTP_GET	TCP: 21		
FTP_PUT	TCP: 21		
NFS	TCP: 111 2049, UDP: 111 2049		
SAMBA	TCP: 139		
SMB	TCP: 445		
TFTP	UDP: 69		
EMAIL			
IMAP	TCP: 143		
IMAPS	TCP: 993		
POP3	TCP: 110		
POP3S	TCP: 995		
SMTP	TCP: 25		
SMTPS	TCP: 465		
NETWORK SERVICES			
BGP	TCP: 179		
DHCP	UDP: 67-68		
DHCP6	UDP: 546 547		
DNS	TCP: 53, UDP: 53		
NTP	TCP: 123, UDP: 123		
OSPF	IP: 89		
PING	ICMP (8:)		
RIP	UDP: 520		
SNMP	TCP: 161-162, UDP: 161-162		
SYSLOG	UDP: 514		
TRACEROUTE	UDP: 33434-33535		
AUTHENTICATION			
KERBEROS	TCP: 88 464, UDP: 88 464		
LDAP	TCP: 389		
LDAP_UDP	UDP: 389		
RADIUS	UDP: 1812 1813		
REMOTE ACCESS			
DCE-RPC	TCP: 135, UDP: 135		
ONC-RPC	TCP: 111, UDP: 111		
PC-Anywhere	TCP: 5631, UDP: 5632		
RDP	TCP: 3389		
SSH	TCP: 22		
TELNET	TCP: 23		

VNC	TCP: 5900	
WINS	TCP: 1512, UDP: 1512	
X-WINDOWS	TCP: 6000-6063	
TUNNELING		
AH	IP: 51	
ESP	IP: 50	
GRE	IP: 47	
IKE	UDP: 500 4500	
L2TP	TCP: 1701, UDP: 1701	
PPTP	TCP: 1723	
SOCKS	TCP: 1080, UDP: 1080	
SQUID	TCP: 3128	
VOIP, MESSAGING & OTHER APPLICATIONS		
H323	TCP: 1720 1503, UDP: 1719	
IRC	TCP: 6660-6669	
MS-SQL	TCP: 1433 1434	
MYSQL	TCP: 3306	
RTSP	TCP: 554 7070 8554, UDP: 554	
SCCP	TCP: 2000	
SIP	TCP: 5060, UDP: 5060	
SIP-MSNmessenger	TCP: 1863	
WEB PROXY		
webproxy	ALL	
UNCATEGORIZED		
AOL	TCP: 5190-5194	disable
CVSPSERVER	TCP: 2401, UDP: 2401	disable
FINGER	TCP: 79	disable
GOPHER	TCP: 70	disable
ICA	TCP: 1494	
INFO_ADDRESS	ICMP (17:)	disable
INFO_REQUEST	ICMP (15:)	disable
Internet-Locator-Service	TCP: 389	disable
MGCP	UDP: 2427 2727	disable
MMS	TCP: 1755, UDP: 1024-5000	disable
NNTP	TCP: 119	disable
NONE	TCP: 0	disable
NetMeeting	TCP: 1720	disable
PING6	ICMP6 (128:)	disable
QUAKE	UDP: 26000 27000 27910 27960	disable
RADIUS-OLD	UDP: 1645 1646	disable
RAUDIO	UDP: 7070	disable
REXEC	TCP: 512	disable
RLOGIN	TCP: 513:512-1023	disable
RSH	TCP: 514:512-1023	disable
Radius-1	UDP: 1645	
Radius-2	UDP: 1812	
TALK	UDP: 517-518	disable
TIMESTAMP	ICMP (13:)	disable
UUCP	TCP: 540	disable
VDOLIVE	TCP: 7000-7010	disable
WAIS	TCP: 210	disable
WINFRAME	TCP: 1494 2598	disable

3.2.2.2 Group

Group Name	Type	Member
Email Access	Firewall	DNS, IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS
Exchange Server	Firewall	DCE-RPC, DNS, HTTPS
Web Access	Firewall	DNS, HTTP, HTTPS
Windows AD	Firewall	DCE-RPC, DNS, KERBEROS, LDAP, LDAP_UDP, SAMBA, SMB
grpRadius	Firewall	Radius-1, Radius-2

3.2.3 Schedule

3.2.3.1 Recurring

Name	Day	Start	Stop
Midday	monday, tuesday, wednesday, thursday, friday	12:00	13:30
always	sunday, monday, tuesday, wednesday, thursday, friday, saturday	00:00	00:00
none		00:00	00:00

3.2.4 Virtual IP

Name	Interface	IP	Port	Map to IP	Port
VIP_svrMail01	wan1	194.191.86.190	4000(tcp)	192.168.1.210	4000(tcp)

3.2.5 IP Pool

Name	Type	External IP Range	Internal IP	ARP Reply
poolOut1	overload	30.30.30.30 - 30.30.30.35		enable

3.3 Traffic Shaping

3.3.1 Traffic Shapers

Shared	Apply	Priority	Maximum (KBps)	Guaranteed (KBps)	DSCP
guarantee-100kbps	per policy	high	1048576	100	-
high-priority	per policy	high	1048576	-	-
low-priority	per policy	low	1048576	-	-
medium-priority	per policy	medium	1048576	-	-
shared-1M-pipe	for all policies	high	1024	-	-

4. Security Profiles

4.1 AntiVirus

4.1.1 Profiles

Profile: default

Comment	Scan files and block viruses.
Inspection Mode	flow-based
Scan Mode	full
Detect Viruses	block

Inspected Protocols

HTTP	SMTP	POP3	IMAP	FTP	NNTP	SMB
enable	enable	enable	enable	enable	disable	disable

Inspection Options

Treat Windows Executables in Email Attachments as Viruses	enable
Include Mobile Malware Protection	enable

Profile: sniffer-profile

Comment	Scan files and monitor viruses.
Inspection Mode	flow-based
Scan Mode	full
Detect Viruses	block

Inspected Protocols

HTTP	SMTP	POP3	IMAP	FTP	NNTP	SMB
enable	enable	enable	enable	enable	disable	disable

Inspection Options

Treat Windows Executables in Email Attachments as Viruses	enable
Include Mobile Malware Protection	enable

4.1.2 Other Anti-Virus Settings

Default DB	extended
Grayware Detection	enable

4.2 Web Filter

Profile: default

Comment	Default web filtering.
Inspection Mode	Flow-based

Fortiguard Categories

Blocked Categories	Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Extremist Groups, Nudity and Risque, Pornography, Dating, Weapons (sales), Unrated, Marijuana, Sex Education, Alcohol, Tobacco, Lingerie and Swimsuit, Sports Hunting and War Games, Malicious Websites, Phishing, Spam URLs, Dynamic DNS
(Allowed Categories	all the rest)

Profile: monitor-all

Comment	Monitor and log all visited URLs, proxy-based.
Inspection Mode	Flow-based

Fortiguard Categories

Monitored Categories	Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Explicit Violence, Extremist Groups, Proxy Avoidance, Plagiarism, Child Abuse, Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Nudity and Risque, Pornography, Dating, Weapons (sales), Marijuana, Sex Education, Alcohol, Tobacco, Lingerie and Swimsuit, Sports Hunting and War Games, Freeware and Software Downloads, File Sharing and Storage, Streaming Media and Download, Peer-to-peer File Sharing, Internet Radio and TV, Internet Telephony, Malicious Websites, Phishing, Spam URLs, Advertising, Brokerage and Trading, Games, Web-based Email, Entertainment, Arts and Culture, Education, Health and Wellness, Job Search, Medicine, News and Media, Social Networking, Political Organizations, Reference, Global Religion, Shopping, Society and Lifestyles, Sports, Travel, Personal Vehicles, Dynamic Content, Meaningless Content, Folklore, Web Chat, Instant Messaging, Newsgroups and Message Boards, Digital Postcards, Child Education, Real Estate, Restaurant and Dining, Personal Websites and Blogs, Content Servers, Domain Parking, Personal Privacy, Finance and Banking, Search Engines and Portals, General Organizations, Business, Information and Computer Security, Government and Legal Organizations, Information Technology, Armed Forces, Web Hosting, Secure Websites, Web-based Applications, Unrated
(Allowed Categories	all the rest)

Profile: no_SocialMedia

Inspection Mode	Flow-based

Fortiguard Categories

Monitored Categories	Extremist Groups, Abortion, Advocacy Organizations, Alcohol, Alternative Beliefs, Dating, Gambling, Lingerie and Swimsuit, Marijuana, Nudity and Risque, Other Adult Materials, Pornography, Sex Education, Sports Hunting and War Games, Tobacco, Weapons (sales), Unrated
Blocked Categories	Dynamic DNS, Malicious Websites, Phishing, Spam URLs, News and Media, Social Networking, Society and Lifestyles
(Allowed Categories	all the rest)

Profile: sniffer-profile

Comment	Monitor web traffic.
Inspection Mode	Flow-based

4.3 DNS Filter

Profile: default

Comment	Default dns filtering.
Block DNS requests to known Botnet C&C	enable
Enforce 'Safe search' on Google,Bing,YouTube	disable

Fortiguard Categories	
Monitored Categories	Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Extremist Groups, Nudity and Risque, Pornography, Dating, Weapons (sales), Unrated, Marijuana, Sex Education, Alcohol, Tobacco, Lingerie and Swimsuit, Sports Hunting and War Games
Blocked Categories	Malicious Websites, Phishing, Spam URLs, Dynamic DNS
(Allowed Categories	all the rest)

Options

Allow DNS requests when a rating error occurs	error-allow
Log all DNS queries and responses	disable
Redirect blocked DNS requests	redirect
Redirect Portal IP	Use FortiGuard Default

4.4 Application Control

Sensor: block-botnet

Categories	Action
Botnet	block
All Other Known Applications	pass
Unknown Applications	pass

Options	
Allow and Log DNS Traffic	enable
QUIC	block
Replacement Messages for HTTP-based Applications	enable

Sensor: block-high-risk

Categories	Action
P2P, Proxy, Botnet	block
All Other Known Applications	pass
Unknown Applications	pass

Options	
Allow and Log DNS Traffic	enable
QUIC	block
Replacement Messages for HTTP-based Applications	enable

Sensor: default

Comment: Monitor all applications.

Categories	Action
(All Categories)	monitor
All Other Known Applications	pass
Unknown Applications	pass

Options	
Allow and Log DNS Traffic	enable
QUIC	block
Replacement Messages for HTTP-based Applications	enable

Sensor: no_Game_Video

Categories	Action
Video/Audio, Proxy, Game	block
All Other Known Applications	monitor
Unknown Applications	pass

Options	
Allow and Log DNS Traffic	enable
QUIC	block
Replacement Messages for HTTP-based Applications	enable

Sensor: sniffer-profile

Comment: Monitor all applications.

Categories	Action
(All Categories)	monitor
All Other Known Applications	pass
Unknown Applications	pass

Options	
Allow and Log DNS Traffic	disable
QUIC	block
Replacement Messages for HTTP-based Applications	enable

4.5 Intrusion Prevention

4.5.1 IPS Sensor

Sensor: all_default

Comment: All predefined signatures with default setting.

Sensor: all_default_pass

Comment: All predefined signatures with PASS action.

Sensor: default

Comment: Prevent critical attacks.

IPS Filter ID	Details	Action	Logging/Packet Log
1	Location: all, OS: all, Application: all, Protocol: all, Severity: medium high critical, Target: all	default	enable/disable

Sensor: high_security

Comment: Blocks all Critical/High/Medium and some Low severity vulnerabilities

IPS Filter ID	Details	Action	Logging/Packet Log
1	Location: all, OS: all, Application: all, Protocol: all, Severity: medium high critical, Target: all	block	enable/disable
2	Location: all, OS: all, Application: all, Protocol: all, Severity: low, Target: all	default	enable/disable

Sensor: protect_client

Comment: Protect against client-side vulnerabilities.

Sensor: protect_email_server

Comment: Protect against email server-side vulnerabilities.

IPS Filter ID	Details	Action	Logging/Packet Log
1	Location: server, OS: all, Application: all, Protocol: SMTP POP3 IMAP, Severity: all, Target: server	default	enable/disable

Sensor: protect_http_server

Comment: Protect against HTTP server-side vulnerabilities.

IPS Filter ID	Details	Action	Logging/Packet Log
1	Location: server, OS: all, Application: all, Protocol: HTTP, Severity: all, Target: server	default	enable/disable

Sensor: sniffer-profile

Comment: Monitor IPS attacks.

IPS Filter ID	Details	Action	Logging/Packet Log
1	Location: all, OS: all, Application: all, Protocol: all, Severity: high critical, Target: all	default	enable/disable

4.6 Anti-Spam

Profile: default

Comment	Malware and phishing URL filtering.
Inspection Mode	flow-based
Scan Mode	full
Spam-Log	enable
Spam Detection and Filtering	disable

Profile: sniffer-profile

Comment	Malware and phishing URL monitoring.
Inspection Mode	flow-based
Scan Mode	full
Spam-Log	enable
Spam Detection and Filtering	disable

4.7 Data Leak Prevention

Sensor: Content_Archive

Inspection Mode	Proxy-based
Protocols to log summary	smtp pop3 imap http-get http-post ftp nntp mapi
Protocols to content archive	smtp pop3 imap http-get http-post ftp nntp mapi

Sensor: Content_Summary

Inspection Mode	Proxy-based
Protocols to log summary	smtp pop3 imap http-get http-post ftp nntp mapi

Sensor: Credit-Card

Inspection Mode Proxy-based

Seq#	Type	Filter	Action	Services	Archive
1	file	Containing credit-card	Log Only	smtp pop3 imap http-get http-post mapi	disable
2	message	Containing credit-card	Log Only	smtp pop3 imap http-post mapi	disable

Sensor: Large-File

Inspection Mode Proxy-based

Seq#	Type	Filter	Action	Services	Archive
1	file	File Size >= 5120 KB	Log Only	smtp pop3 imap http-get http-post mapi	disable

Sensor: SSN-Sensor

Comment	Match SSN numbers but NOT WebEx invite emails.
Inspection Mode	Proxy-based

Seq#	Type	Filter	Action	Services	Archive
1	message	Regular Expression: WebEx	Allow	smtp pop3 imap mapi	disable
2	message	Containing ssn	Log Only	smtp pop3 imap mapi	disable
3	file	Containing ssn	Log Only	smtp pop3 imap http-get http-post ftp mapi	disable

Sensor: default

Comment	Default sensor.
Inspection Mode	Proxy-based

Sensor: sniffer-profile

Comment	Log a summary of email and web traffic.
Inspection Mode	Flow-based
Protocols to log summary	smtp pop3 imap http-get http-post

4.8 VoIP

Profile: default

Comment: Default VoIP profile.

VoIP Filtering	
SIP	
Limit REGISTER request	0 (requests/sec/policy)
Limit INVITE request	0 (requests/sec/policy)
RTP	enable
Logging	enable
Logging of violations	disable
Block unknown commands	enable
SCCP	
Limit Call Setup	0 (Calls/min/client)
Logging	disable
Logging of violations	disable

Profile: strict

VoIP Filtering	
SIP	
Limit REGISTER request	0 (requests/sec/policy)
Limit INVITE request	0 (requests/sec/policy)
RTP	enable
Logging	enable
Logging of violations	disable
Block unknown commands	enable
SCCP	
Limit Call Setup	0 (Calls/min/client)
Logging	disable
Logging of violations	disable

4.9 ICAP

Profile Name: default

Option	Status	Server	On failure
Request Processing	disable	--	error
Response Processing	disable	--	error
Streaming Media Bypass	disable	--	--

4.10 Web Application Firewall Profiles

Profile: default

Signature enabled	Action	Severity
Bad Robot	allow	high
SQL Injection	block	high
Generic Attacks	block	high
Trojans	block	high
Information Disclosure	allow	low
Known Exploits	block	high

Constraint enabled	Limit	Action	Severity
content-length	67108864	allow	low
header-length	8192	allow	low
line-length	1024	allow	low
max-cookie	16	allow	low
max-header-line	32	allow	low
max-range-segment	5	allow	high
max-url-param	16	allow	low
param-length	8192	allow	low
url-param-length	8192	allow	low

4.11 FortiClient Profiles

Profile: default

Endpoint Vulnerability Scan on Client

Vulnerability quarantine level	high
Non-compliance action	warning

System Compliance

Minimum FortiClient version	disable
Upload Logs to FortiAnalyzer	traffic vulnerability event
Non-compliance-action	warning

4.12 Proxy Options

Profile: default

Comment: All default services.
RPC over HTTP: enable

Protocol Port Mapping

Protocol	Status	Inspection Port
http	enable	80
smtp	enable	25
pop3	enable	110
imap	enable	143
ftp	enable	21
nntp	enable	119
mapi	enable	135
dns	enable	53

Options

Common Options	Comfort Client	disable
	Block Oversized File/Email	disable
Web Options	Chunked Bypass	disable
	Add Fortinet Bar	disable
	HTTP Policy Redirect	disable
Email Options	Allow Fragmented Messages	enable
	Append Signature (SMTP)	disable

4.13 SSL Inspection

4.13.1 certificate-inspection

Comment: SSL handshake inspection.

SSL Inspection Options

Enable SSL Inspection of	Multiple Clients Connecting to Multiple Servers
Inspection Method	SSL Certificate Inspection
CA Certificate	Fortinet_CA_SSL
Untrusted SSL Certificates	allow

Protocol Port Mapping

Inspect all ports disable

Protocol	Status	Inspection Port
https	certificate-inspection	443

Common Options

Allow Invalid SSL Certificate	disable
Log SSL anomalies	enable

4.13.2 deep-inspection

Comment: Deep inspection.

SSL Inspection Options

Enable SSL Inspection of	Multiple Clients Connecting to Multiple Servers
Inspection Method	Full SSL Inspection
CA Certificate	Fortinet_CA_SSL
Untrusted SSL Certificates	allow
RPC over HTTPS	disable

Protocol Port Mapping

Inspect all ports disable

Protocol	Status	Inspection Port
https	deep-inspection	443
smtps	deep-inspection	465
pop3s	deep-inspection	995
imaps	deep-inspection	993
ftps	deep-inspection	990

Exempt from SSL Inspection

Reputable Websites	disable
Web Categories	Finance and Banking, Health and Wellness
Addresses	android, apple, appstore, citrix, eease, google-drive, google-play, google-play2, google-play3, Gotomeeting, microsoft, update.microsoft.com, adobe, Adobe Login, dropbox.com, fortinet, googleapis.com, icloud, itunes, skype, swscan.apple.com, verisign, Windows update 2, auth.gfx.ms, autoupdate.opera.com, softwareupdate.vmware.com, firefox update server
Log SSL exemptions	disable

Common Options

Allow Invalid SSL Certificate	disable
Log SSL anomalies	enable

4.14 Advanced Settings

4.14.1 Custom Categories

Custom Category Name
custom1
custom2

5. VPN

5.1 IPSec

5.1.1 AutoKey - Interface Mode

5.1.1.1 Dialup

Comment: VPN: Dialup (Created by VPN wizard)
Wizard-Type: dialup-forticlient

Network

Remote Gateway	Dialup User
Local Interface	wan1
Mode Config	enable
Client Address Range	10.10.10.5-10.10.10.150 / 255.255.255.0
Use System DNS	enable
Split Tunneling	enable - Accessible Networks: LAN
NAT Traversal	enable - keepalive 10 sec.
Dead Peer Detection	on-demand - Retries: 3, Interval: 20

Authentication

Method	Pre-shared Key
IKE Version	1
IKE Mode	aggressive
Peer Type	any

Phase 1 Proposal

Proposal	aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-sha1
Diffie-Hellman Groups	14 5
Key Lifetime	86400 sec

XAUTH

Type	auto
User Group	Sales

Phase 2 Settings

Dialup	Selectors	Local: 0.0.0.0/0 (Subnet) - Remote: 0.0.0.0/0 (Subnet)
	Proposal	aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256 3des-sha256
	Replay Detection	enable
	PFS	enable - DH Groups: 14 5
	Key Life	43200 sec
	Auto-Negotiate	disable
	Keep-Alive	disable
	Comments	VPN: Dialup (Created by VPN wizard)

5.1.1.2 SitetoSite

Comment: VPN: SitetoSite (Created by VPN wizard)
Wizard-Type: static-fortigate

Network

Remote Gateway	1.2.3.4 (Static IP)
Local Interface	wan1
Mode Config	disable
NAT Traversal	enable - keepalive 10 sec.
Dead Peer Detection	on-demand - Retries: 3, Interval: 20

Authentication

Method	Pre-shared Key
IKE Version	1
IKE Mode	main
Peer Type	any

Phase 1 Proposal

Proposal	aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-sha1
Diffie-Hellman Groups	14 5
Key Lifetime	86400 sec

Phase 2 Settings

SitetoSite	Selectors	Local: 192.168.1.0/24 (Subnet) - Remote: 10.10.15.0/24 (Subnet)
	Proposal	aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256 3des-sha256
	Replay Detection	enable
	PFS	enable - DH Groups: 14 5
	Key Life	43200 sec
	Auto-Negotiate	disable
	Keep-Alive	disable
	Comments	VPN: SitetoSite (Created by VPN wizard)

5.2 SSL

5.2.1 Portals

5.2.1.1 full-access

Tunnel Mode	**enable**
Split Tunneling	disable
Source IP Pools	SSLVPN_TUNNEL_ADDR1

IPv6 Tunnel Mode	**enable**
Split Tunneling	disable
Source IPv4 Pools	SSLVPN_TUNNEL_IPv6_ADDR1

Tunnel Mode Client Options

Allow client to save password	disable
Allow client to connect automatically	disable
Allow client to keep connections alive	disable

Web Mode	**enable**
Portal Message	Welcome to SSL VPN Service
Theme	blue
Show Session Information	enable
Show Connection Launcher	enable
Show Login History	enable - Number of History Entries: 5
User Bookmarks	enable

5.2.1.2 web-access

Tunnel Mode	**disable**

Web Mode	**enable**
Portal Message	Welcome to SSL VPN Service
Theme	blue
Show Session Information	enable
Show Connection Launcher	enable
Show Login History	enable - Number of History Entries: 5
User Bookmarks	enable

5.2.1.3 tunnel-access

Tunnel Mode	**enable**
Split Tunneling	disable
Source IP Pools	SSLVPN_TUNNEL_ADDR1

IPv6 Tunnel Mode	**enable**
Split Tunneling	disable
Source IPv4 Pools	SSLVPN_TUNNEL_IPv6_ADDR1

Tunnel Mode Client Options	
Allow client to save password	disable
Allow client to connect automatically	disable
Allow client to keep connections alive	disable

Web Mode	**disable**

5.2.2 Settings

Connection Settings

Listen on Interface(s)	wan1
Listen on Port	10443
Restrict Access	Allow access from any host
Idle Logout	Logout users when inactive for specified period: 300 (Seconds)
Login Timeout	30 sec
DTLS Hello Timeout	10 sec
Server Certificate	Fortinet_Factory
Require Client Certificate	disable

Tunnel Mode Client Settings

Address Range	SSLVPN_TUNNEL_ADDR1
DNS-Server	Same as client system DNS
Allow Endpoint Registration	disable

Authentication	Realm	Portal
Sales		full-access
All Other Users/Groups		web-access

Other Settings

Allowed Protocols	sv1-2
Algorithm	default
Authentication Timeout	28800 sec
HTTP Request Header Timeout	20 sec
HTTP Request Body Timeout	30 sec
Port Precedence (over HTTPS)	enable
Auto Tunnel Static Route	enable
Login Attempt Limit	2
Login Block Time	60 sec

6. User & Device

6.1 Users

6.1.1 User Definition

User Name	Type	Two-Factor	Status	Contact Info
Hans Muster	Local	-	enable	
Max Muster	Local	FortiToken (FTKMOB39D4B5CCE0)	enable	max.muster@gmx.ch
guest	Local	-	enable	

6.1.2 User Groups

Group Name	Type	Members	Additional
Guest-group	firewall	guest	
SSO_Guest_Users	firewall		
Sales	firewall	Hans Muster, Max Muster	

6.2 Device

6.2.1 Custom Device Groups

Group Name	Members	Comment
Mobile Devices	android-phone, android-tablet, blackberry-phone, blackberry-playbook, ipad, iphone, windows-phone, windows-tablet	Phones, tablets, etc.
Network Devices	fortinet-device, other-network-device, router-nat-device	Routers, firewalls, gateways, etc.
Others	gaming-console, media-streaming	Other devices.

6.3 Authentication

6.3.1 LDAP Server

Name	Server Name/IP	Port	CN Identifier	Distinguished Name
svrDC01	192.168.52.200	389	cn	CN=Users,DC=test,DC=local
	Bind Type	regular (Filter: (&(objectcategory=group)(member=*)), User DN: Administrator)		

6.3.2 Radius Server

Name	Type	Primary Server Name/IP (Secondary)
svrRAD01	query	192.168.52.205

6.3.3 Settings

Parameter	Value
Authentication Timeout	5 minutes
Protocol Support	http, https, ftp, telnet
Certificate	Fortinet_Factory

6.4 FortiTokens

S/N	Status	User	Comment
FTKMOB3952C93E46	active	monitor	
FTKMOB39D4B5CCE0	active	{Max Muster}	

7. WiFi & Switch Controller

7.1 WiFi Controller

7.1.1 SSID

guest	Tunnel to Wireless Controller
SSID	guest
Security Mode	wpa2-only-personal
Data Encryption	AES
Broadcast SSID	enable
Schedule	always
Detect and Identify Devices	enable

work	Tunnel to Wireless Controller
SSID	work
Security Mode	wpa2-only-enterprise
Data Encryption	AES
Authentication	Radius Server: svrRAD01
Broadcast SSID	enable
Schedule	always
Detect and Identify Devices	enable

7.1.2 FortiAP Profiles

FAPU423E-default

Platform	FAPU423E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPU421E-default

Platform	FAPU421E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAP423E-default

Platform	FAP423E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAP421E-default

Platform	FAP421E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS423E-default

Platform	FAPS423E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS422E-default

Platform	FAPS422E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS421E-default

Platform	FAPS421E
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS323CR-default

Platform	FAPS323CR
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS322CR-default

Platform	FAPS322CR
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS321CR-default

Platform	FAPS321CR
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

FAPS322C-default

Platform	FAPS322C
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	802.11ac/n/a
Channel Width	20MHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

AP-11N-default

Platform	FAPAP-11N
Country	US
Radio-1	Access Point
Band	802.11n/g/b at 2.4GHz
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs
Radio-2	Access Point
Band	
Channel	
TX Power	100%
SSIDs	Automatically assign Tunnel-mode SSIDs

7.1.3 WIDS Profiles

default	**Default WIDS profile.**
Rogue AP Detection	enable
Background Scan Every	600 seconds
Intrusion Detection Settings	
Asleap Attack	enable
Association Frame Flooding	enable (Threshold: 30, Interval: 10 sec)
Authentication Frame Flooding	enable (Threshold: 30, Interval: 10 sec)
Broadcasting De-authentication	enable
EAPOL-FAIL Flooding (to AP)	enable (Threshold: 10, Interval: 1 sec)
EAPOL-LOGOFF Flooding (to AP)	enable (Threshold: 10, Interval: 1 sec)
EAPOL-START Flooding (to AP)	enable (Threshold: 10, Interval: 1 sec)
EAPOL-SUCC Flooding (to AP)	enable (Threshold: 10, Interval: 1 sec)
Invalid MAC OUI	enable
Long Duration Attack	enable (Threshold: 8200 usec)
Null SSID Probe Response	enable
Premature EAPOL-FAIL Flooding (to Client)	enable (Threshold: 10, Interval: 1 sec)
Premature EAPOL-SUCC Flooding (to Client)	enable (Threshold: 10, Interval: 1 sec)
Spoofed De-authentication	enable
Weak WEP IV (Initialization Vector)	enable
Wireless Bridge	enable

default-wids-apscan-enabled

Rogue AP Detection	enable
Background Scan Every	600 seconds
Intrusion Detection Settings	

7.1.4 Settings

Manage cloud-based FortiAPs	disable
Duplicate SSID	disable

7.2 FortiSwitch Controller

7.2.1 FortiSwitch Ports

S124DP3X15000237

WAN1 peer port	internal7
WAN1 admin status	enable
Managed Switch Profile	default

Port	Description	Native VLAN	Allowed VLANs	Speed	IGMP Snooping	DHCP Blocking	Loop Guard	STP
port1		VLAN30		auto	disable	untrusted	disabled	enabled
port2		VLAN30		auto	disable	untrusted	disabled	enabled
port3		VLAN30		auto	disable	untrusted	disabled	enabled
port4		VLAN30		auto	disable	untrusted	disabled	enabled
port5		VLAN30		auto	disable	untrusted	disabled	enabled
port6		VLAN30		auto	disable	untrusted	disabled	enabled
port7		VLAN30		auto	disable	untrusted	disabled	enabled
port8		VLAN30		auto	disable	untrusted	disabled	enabled
port9		VLAN30		auto	disable	untrusted	disabled	enabled
port10		VLAN30		auto	disable	untrusted	disabled	enabled
port11		VLAN30		auto	disable	untrusted	disabled	enabled
port12		VLAN30		auto	disable	untrusted	disabled	enabled
port13		VLAN40		auto	disable	untrusted	disabled	enabled
port14		VLAN40		auto	disable	untrusted	disabled	enabled
port15		VLAN40		auto	disable	untrusted	disabled	enabled
port16		VLAN40		auto	disable	untrusted	disabled	enabled
port17		VLAN40		auto	disable	untrusted	disabled	enabled
port18		VLAN40		auto	disable	untrusted	disabled	enabled
port19		VLAN40		auto	disable	untrusted	disabled	enabled
port20		VLAN40		auto	disable	untrusted	disabled	enabled
port21		VLAN40		auto	disable	untrusted	disabled	enabled
port22		VLAN40		auto	disable	untrusted	disabled	enabled
port23		VLAN40		auto	disable	untrusted	disabled	enabled
port24		vsw.internal7		auto	disable	untrusted	disabled	enabled
port25		vsw.internal7		auto	disable	untrusted	disabled	enabled
port26		vsw.internal7		auto	disable	untrusted	disabled	enabled
All other ports	vsw.root							

7.2.2 FortiSwitch VLANs

VLAN Name	VLAN ID	IP/Netmask	Access	Description
vsw.internal7	1	0.0.0.0/0	-	-
VLAN30	30	10.10.30.99/24	-	-
VLAN40	40	10.10.40.99/24	-	-

7.2.3 Spanning-Tree global

Name	
Revision	0
Hello-Time	2
forward-time	15
Max-Age	20
Max-Hops	20

7.2.4 FortiSwitch Storm Control

Rate	500
Unknown-Unicast	enable
Unknown-Multicast	disable
Broadcast	enable

8. Log

8.1 Log Setting

Local Log

Memory	enable
Severity	information

Reports

Enable Local Reports	enable
Enable Historical FortiView	enable

FortiAnalyzer/FortiManager	enable
IP Address	192.168.1.160
Severity	information
Upload Option	realtime
Encrypt Log Transmission	disable
Certificate	

FortiCloud	enable
Account	fortinet@boll.ch
Severity	information
Upload Option	realtime

8.2 Other Log Settings

Event Category	Log
System activity event	enable
Router activity event	enable
VPN activity event	enable
User activity event	enable
Endpoint event	enable
HA event	enable
Explicit web proxy event	enable
WiFi activity event	enable
PCI DSS compliance check	enable
Security Fabric Audit	enable
Switch-Log	enable

Local Traffic Logging

Log Denied Unicast Traffic	disable
Log Allowed Traffic	disable
Log Local Out Traffic	disable
Log Denied Broadcast Traffic	disable

GUI Preferences

Display Logs/FortiView from	fortianalyzer
Resolve hostnames	enable
Resolve unknown applications	enable

8.3 Threat Weight

Log Threat Weight

Application Protection

Botnet Applications	disable
P2P Applications	low
Proxy Applications	medium
Games Applications	disable

Intrusion Protection

Critical Severity Attack Detected	critical
High Severity Attack Detected	high
Medium Severity Attack Detected	medium
Low Severity Attack Detected	low
Informational Severity Attack Detected	disable

Malware Protection

Malware	critical
Botnet C&C Communication	critical

Packet Based Inspection

Blocked by Firewall Policy	high
Failed Connection Attempts	low

Web Activity

All Blocked URLs	high
Malicious Websites	high
Phishing	high
Spam URLs	high
Drug Abuse	medium
Hacking	medium
Illegal or Unethical	medium
Discrimination	medium
Explicit Violence	medium
Extremist Groups	medium
Proxy Avoidance	medium
Plagiarism	medium
Child Abuse	medium
Peer-to-peer File Sharing	low
Pornography	low

Risk Level Values

Low	5
Medium	10
High	30
Critical	50