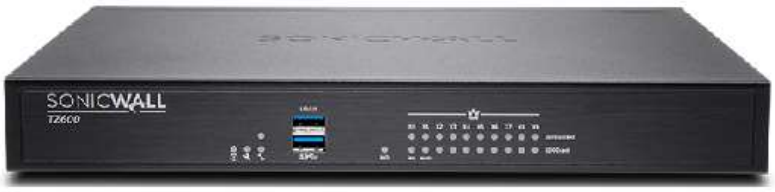
SonicWALL Configuration Report

Hostname: 0017C50FA94C



Firmware Version: 5.8.0.0-10o

Table of Contents

Report printed on DESKTOP-R0JBCCS at 01/23/19 16:10:02 with autodoc version 10.06

1. System

0017C50FA94C (TZ600)

- HA Port — Unused
- X1 — WAN — 192.168.1.157 —  192.168.1.129
- X0 — LAN — 192.168.168.168
- X2
- X3
- X4
- X5
- X6
- X7
- X8
- U0
- U1

1.1 Administration

Firewall Name

Firewall Name	0017C50FA94C (TZ600)

Login Security

Enforce a minimum password length of	1
Apply these password contraints for	Administrator = on Other full administrators = on Limited administrators = on Other local users = on
Log out the administrator after inactivity of (minutes)	60
Enable administrator/user lockout	off
Failed login attempts per minute before lockout	5
Lockout Period (minutes)	5

Multiple Administrators

On preemption by another administrator	Drop to non-config mode
Allow preemption by a lower priority administrator after inactivity of (minutes)	10

Web Management Settings

HTTP / HTTP Management Port	80 / 80
HTTPS / HTTPS Management Port	443 / 443
Certificate Selection	Use Selfsigned Certificate
Certificate Common Name	192.168.168.168
Default Table Size	50 items per page
Auto-updated Table Refresh Interval	10 in seconds
Enable Tooltip	on
Form Tooltip Delay	2000 in msecs
Form Tooltip Delay	3000 in msecs
Text Tooltip Delay	500 in msecs

Front-Panel Administrative Interface

Enable front-panel Administrative interface	on
Require PIN for front-panel access	
PIN	
LCD idle timer	60

SSH Management Settings

SSH Management Port	22

Advanced Management

Enable SNMP	off
Enable management using GMS	off

Download URL

Manually specify GVC Download URL (http://)	help.mysonicwall.com/applications/vpnclient/

Language

Language Selection	English

1.2 Time

Timezone	Europe (GMT+1:00)
Set time automatically using NTP	on
Automatically adjust clock for daylight saving time	on
Display UTC in logs (instead of local time)	off
Display Date in international format	off
Update internval (minutes)	60

1.3 Schedules

Name	Days of Week	Time
Work Hours		
	M-T-W-TH-F	08:00-17:00
After Hours		
	M-T-W-TH-F	00:00-08:00
	M-T-W-TH-F	17:00-24:00
	SA-SU	00:00-24:00
Weekend Hours		
	SA-SU	00:00-24:00

1.4 Settings

Firmware Auto-Update	
Enable Firmware Auto-Update	on
Download new firmware automatically when available	off

FIPS	
Enable FIPS Mode	off

1.5 Diagnostics

Tech Support Report	
Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall	on
Time Interval (minutes)	1440

2. Network

2.1 Interfaces

Name	Zone	IP Address	Subnet Mask	IP Assignment	Comment
X0	LAN	192.168.168.168	255.255.255.0	Static	Default LAN
X1	WAN	192.168.1.157	255.255.255.192	Static	Default WAN
X2				N/A	
X3				N/A	
X4				N/A	
X5				N/A	
X6				N/A	
X7				N/A	
X8				N/A	
U0				N/A	
U1				N/A	

2.1.1 Interface 'X0' Settings

Zone	LAN
IP Assignment	Static
Mode	
IP Address	192.168.168.168
Subnet Mask	255.255.255.0
Comment	Default LAN
Management	
- HTTP	Enabled
- HTTPS	Enabled
- Ping	Enabled
- SNMP	Disabled
- SSH	Enabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:4C
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.2 Interface 'X1' Settings

Zone	WAN
IP Assignment	Static
IP Address	192.168.1.157
Subnet Mask	255.255.255.192
Default Gateway	192.168.1.129
DNS Server 1	192.168.1.224
DNS Server 2	192.168.1.225
Comment	Default WAN
Management	
- HTTP	Disabled
- HTTPS	Enabled
- Ping	Enabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:4D
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	on
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.3 Interface 'X2' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:4E
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.4 Interface 'X3' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:4F
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.5 Interface 'X4' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:50
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.6 Interface 'X5' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:51
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.7 Interface 'X6' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:52
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.8 Interface 'X7' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:53
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.9 Interface 'X8' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:54
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.10 Interface 'U0' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	
MAC Address	00:17:C5:0F:A9:55
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.1.11 Interface 'U1' Settings

Zone	
IP Assignment	N/A
Comment	
Management	
- HTTP	Disabled
- HTTPS	Disabled
- Ping	Disabled
- SNMP	Disabled
- SSH	Disabled
User Login	
- HTTP	Disabled
- HTTPS	Disabled
Add rule to enable redirect from HTTP to HTTPS	Enabled

Advanced Settings

Link Speed	Auto Negotiate
MAC Address	00:17:C5:0F:A9:56
Override Default MAC Address	off
Enable flow reporting	on
Enable Multicast Support	off
Enable 802.1p tagging	off
Interface MTU	1500
Fragment non-VPN outbound packets larger than MTU	off
Ignore Don't Fragment (DF) Bit	off
Do not send ICMP Fragmentation Needed...	off
Do not send ICMP Fragmentation Needed...	off

Bandwidth Management

Enable Egress Bandwidth Management	off
Available Interface Egress Bandwidth (Kbps)	384.000
Enable Ingress Bandwidth Management	off
Available Interface Ingress Bandwidth (Kbps)	384.000

2.2 WAN Failover & LB

Enable Load Balancing	on
Respond to Probes	off

2.2.1 Groups

2.2.1.1 Default LB Group

General

Type	Basic Failover Preempt and failback to preferred interfaces when possible

Probing

Check Interface every	5 sec
Deactivate Interface after	6 missed intervals
Reactivate Interface after	3 successful intervals

Interfaces		Probing
U0	Final Back-Up	Physical Monitoring Only
X1		Succeeds Always (no probing).

2.3 Zones

Name	Security Type	Member Interfaces
LAN	Trusted	X0

Allow Interface Trust	yes
Enforce Content Filtering Service	yes
CFS Policy	
Enable Client AV Enforcement Service	no
Enable Gateway Anti-Virus Service	yes
Enable IPS	yes
Enable App Control Service	yes
Enable Anti-Spyware Service	yes
Enforce Global Security Clients	no
Create Group VPN	no
Enable SSL Control	no
Enable SSLVPN Access	no

Name	Security Type	Member Interfaces
WAN	Untrusted	X1

Allow Interface Trust	no
Enforce Content Filtering Service	no
CFS Policy	
Enable Client AV Enforcement Service	no
Enable Gateway Anti-Virus Service	yes
Enable IPS	yes
Enable App Control Service	yes
Enable Anti-Spyware Service	yes
Enforce Global Security Clients	no
Create Group VPN	yes
Enable SSL Control	no
Enable SSLVPN Access	no

Name	Security Type	Member Interfaces
DMZ	Public	N/A

Allow Interface Trust	yes
Enforce Content Filtering Service	yes
CFS Policy	
Enable Client AV Enforcement Service	no
Enable Gateway Anti-Virus Service	no
Enable IPS	no
Enable App Control Service	no
Enable Anti-Spyware Service	no
Enforce Global Security Clients	no
Create Group VPN	no
Enable SSL Control	no
Enable SSLVPN Access	no

Name	Security Type	Member Interfaces
VPN	Encrypted	N/A

Allow Interface Trust	no
Enforce Content Filtering Service	no
CFS Policy	
Enable Client AV Enforcement Service	no
Enable Gateway Anti-Virus Service	no
Enable IPS	no
Enable App Control Service	no
Enable Anti-Spyware Service	no
Enforce Global Security Clients	no
Create Group VPN	no
Enable SSL Control	no
Enable SSLVPN Access	no

Name	Security Type	Member Interfaces		
SSLVPN		N/A		
			Allow Interface Trust	no
			Enforce Content Filtering Service	no
			CFS Policy	
			Enable Client AV Enforcement Service	no
			Enable Gateway Anti-Virus Service	no
			Enable IPS	no
			Enable App Control Service	no
			Enable Anti-Spyware Service	no
			Enforce Global Security Clients	no
			Create Group VPN	no
			Enable SSL Control	no
			Enable SSLVPN Access	yes

Name	Security Type	Member Interfaces		
MULTICAST	Untrusted	N/A		
			Allow Interface Trust	no
			Enforce Content Filtering Service	no
			CFS Policy	
			Enable Client AV Enforcement Service	no
			Enable Gateway Anti-Virus Service	no
			Enable IPS	no
			Enable App Control Service	no
			Enable Anti-Spyware Service	no
			Enforce Global Security Clients	no
			Create Group VPN	no
			Enable SSL Control	no
			Enable SSLVPN Access	no

Name	Security Type	Member Interfaces		
WLAN	Wireless	N/A		
			Allow Interface Trust	no
			Enforce Content Filtering Service	no
			CFS Policy	
			Enable Client AV Enforcement Service	no
			Enable Gateway Anti-Virus Service	no
			Enable IPS	no
			Enable App Control Service	no
			Enable Anti-Spyware Service	no
			Enforce Global Security Clients	no
			Create Group VPN	yes
			Enable SSL Control	no
			Enable SSLVPN Access	no

2.4 DNS

DNS Server	Address
DNS Server 1	0.0.0.0
DNS Server 2	0.0.0.0
DNS Server 3	0.0.0.0

2.5 Address Objects

2.5.1 Address Groups

#	Name	Members
1	All Authorized Access Points	
2	All Interface IP	"LAN Primary IP", "WAN Primary IP", "X2 IP", "X3 IP", "X4 IP", "X5 IP", "X6 IP", "X7 IP", "X8 IP", "U0 IP"
3	All SonicPoints	
4	All U0 Management IP	"U0 IP"
5	All WAN IP	"WAN Primary IP"
6	All X0 Management IP	
7	All X1 Management IP	
8	All X2 Management IP	"X2 IP"
9	All X3 Management IP	"X3 IP"
10	All X4 Management IP	"X4 IP"
11	All X5 Management IP	"X5 IP"
12	All X6 Management IP	"X6 IP"
13	All X7 Management IP	"X7 IP"
14	All X8 Management IP	"X8 IP"
15	Default SonicPoint ACL Allow Group	
16	Default SonicPoint ACL Deny Group	
17	Default Trusted Relay Agent List	
18	DMZ Interface IP	
19	DMZ Subnets	
20	Firewalled Subnets	"LAN Subnets", "DMZ Subnets", "WLAN Subnets"
21	Guest Authentication Servers	
22	LAN Interface IP	"LAN Primary IP"
23	LAN Subnets	"LAN Primary Subnet"
24	Node License Exclusion List	
25	Public Mail Server Address Group	
26	RBL User Black List	
27	RBL User White List	
28	Richard-Gruppe	"All WAN IP", "X7 Subnet", "U0 Subnet", "Secondary Default Gateway"
29	SonicWALL SSO Agents	
30	SonicWALL Terminal Services Agents	
31	WAN Interface IP	"WAN Primary IP"
32	WAN Subnets	"WAN Primary Subnet"
33	WLAN Interface IP	
34	WLAN Subnets	

2.5.2 Address Objects

#	Name	Address Detail	Type	Zone
1	Default Active WAN IP	192.168.1.157/255.255.255.255	Host	WAN
2	Default Gateway	0.0.0.0/255.255.255.255	Host	WAN
3	Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	
4	Secondary Default Gateway	0.0.0.0/255.255.255.255	Host	WAN
5	U0 IP	0.0.0.0/255.255.255.255	Host	
6	U0 Subnet	0.0.0.0/255.255.255.0	Network	
7	WAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN
8	WLAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN
9	X0 IP	192.168.168.168/255.255.255.255	Host	LAN
10	X0 Subnet	192.168.168.0/255.255.255.0	Network	LAN
11	X1 Default Gateway	192.168.1.129/255.255.255.255	Host	WAN
12	X1 IP	192.168.1.157/255.255.255.255	Host	WAN
13	X1 Subnet	192.168.1.128/255.255.255.192	Network	WAN
14	X2 IP	0.0.0.0/255.255.255.255	Host	
15	X2 Subnet	0.0.0.0/255.255.255.0	Network	
16	X3 IP	0.0.0.0/255.255.255.255	Host	
17	X3 Subnet	0.0.0.0/255.255.255.0	Network	
18	X4 IP	0.0.0.0/255.255.255.255	Host	
19	X4 Subnet	0.0.0.0/255.255.255.0	Network	
20	X5 IP	0.0.0.0/255.255.255.255	Host	
21	X5 Subnet	0.0.0.0/255.255.255.0	Network	
22	X6 IP	0.0.0.0/255.255.255.255	Host	
23	X6 Subnet	0.0.0.0/255.255.255.0	Network	
24	X7 IP	0.0.0.0/255.255.255.255	Host	
25	X7 Subnet	0.0.0.0/255.255.255.0	Network	
26	X8 IP	0.0.0.0/255.255.255.255	Host	
27	X8 Subnet	0.0.0.0/255.255.255.0	Network	

2.6 Services

see Chapter Firewall / Services

2.7 Routing

Use Advanced Routing: off

2.7.1 Dynamic Routing

2.7.1.1 RIP

Default Metric	
Administrative Distance	120
Originate Default Route	off
Redistribute Static Routes	off, metric=
Redistribute Connected Networks	off, metric=
Redistribute OSPF Routes	off, metric=
Redistribute Remote VPN Networks	off, metric=

Interface	Zone	Mode	Receive	Send	Split Horizon	Poison Reverse	Password
X0	LAN	Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X1	WAN	Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X2		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X3		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X4		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X5		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X6		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X7		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
X8		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
U0		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX
U1		Disabled	RIPv2	RIPv2	on	on	XXXXXXXX

2.7.1.2 OSPF

OSPF Router-ID	10.0.0.1
Default Metric	
ABR Type	Cisco
Auto-Cost Reference BW (Mb/s)	
Originate Default Route	?
Metric / Metric Type	10 / External Type 2

		Tag	Metric	Metric Type
Redistribute Static Routes	off			External Type 2
Redistribute Connected Networks	off			External Type 2
Redistribute RIP Routes	off			External Type 2
Redistribute Remote VPN Networks	off			External Type 2

Interface	Zone	Mode	Dead	Hello	Area	Cost	Prio	Auth	Password
X0	LAN	Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X1	WAN	Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X2		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X3		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X4		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X5		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X6		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X7		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
X8		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX
U0		Disabled	40	10	0 (normal)	(auto)	1	disabled	XXXXXXXX

U1		Disabled	40	10	0 (normal)		(auto)	1	disabled	XXXXXXXX

2.7.2 Static Routing

Source	Destination	Service	Gateway	Iface	Metric	Prio	Comment

2.8 NAT Policies

#	Source		Destination		Service		Src Int.	Dst. Int.	Enable	Comment
	Original	Translated	Original	Translated	Original	Translated				
1	Any	Original	WAN Primary IP	Original	Ping	Original	X1	X1	1	Management NAT Policy
2	Any	Original	WAN Primary IP	Original	HTTPS Management	Original	X1	X1	1	Management NAT Policy
3	Any	Original	WAN Primary IP	Original	HTTP Management	Original	X1	X1	1	Management NAT Policy
4	Any	Original	LAN Primary IP	Original	Ping	Original	X0	X0	1	Management NAT Policy
5	Any	Original	LAN Primary IP	Original	SSH Management	Original	X0	X0	1	Management NAT Policy
6	Any	Original	LAN Primary IP	Original	HTTPS Management	Original	X0	X0	1	Management NAT Policy
7	Any	Original	LAN Primary IP	Original	HTTP Management	Original	X0	X0	1	Management NAT Policy
8	Any	Original	LAN Primary IP	Original	ZebTelnet	Original	X0	X0	1	Management NAT Policy
9	Any	Original	LAN Primary IP	Original	Telnet	Original	X0	X0	1	Management NAT Policy
10	All Interface IP	WAN Primary IP	Any	Original	Any	Original	Any	X1	1	Auto-added X1 Default NAT Policy
11	Any	WAN Primary IP	Any	Original	Any	Original	X0	X1	1	Auto-added X0 outbound NAT Policy for X1 WAN

2.9 MAC-IP Anti-spoof

Interface	Enforced	Enable	ARP Lock	ARP Watch	Static ARP	DHCP Server	DHCP Relay	Spoof Detection	Allow Management

2.9.1 Anti-Spoof Cache

No entries.

2.10 DHCP Server

DHCP Server Settings	
Enable DHCP Server	on
Enable Conflict Detection	on
Enable DHCP Server Network Pre-Discovery	off
Enable DHCP Server Persistence	on

2.10.1 DHCP Server Lease Scopes

#	Type	Lease Scope	Interface	Enabled
1	Dynamic	Range: 192.168.168.1 - 192.168.168.167	X0	off

2.10.2 Dynamic Scope 1

Dynamic DHCP Scope Settings

Enable	on
Range Start	192.168.168.1
Range End	192.168.168.167
Lease Time (minutes)	1440
Gateway Preferences	off
Default Gateway	192.168.168.168
Subnet Mask	255.255.255.0
Allow BOOTP Clients to use Range	off

DNS Servers

Domain Name	
	Inherit DNS Settings Dynamically from the SonicWALL's DNS settings
DNS Server 1	192.168.1.224
DNS Server 2	192.168.1.225
DNS Server 3	0.0.0.0

WINS Servers

WINS Server 1	0.0.0.0
WINS Server 2	0.0.0.0

VoIP Call Managers

Call Manager 1	
Call Manager 2	
Call Manager 3	

DHCP Generic Options

DHCP Generic Option Group	
Send Generic options always	off

2.11 IP Helper

Enable IP Helper	off
Enable DHCP Support	
Enable Netbios Support	

2.12 Web Proxy

Proxy Web Server Name	
Proxy Web Server	
Proxy Web Server Port	0
Bypass Proxy Servers Upon Proxy Server Failure	off
Forward Public Zone Client Requests to Proxy Server	off

2.13 Network Monitor

Not configured.

3. SonicPoint

3.1 Provisioning Profiles

3.1.1 SonicPoint

Eanble SonicPoint	1
Enable RF Monitoring	0
Name Prefix	SonicPoint
Country Code	US
802.11n Radio Virtual AP Group	
802.11g Radio Virtual AP Group	
802.11a Radio Virtual AP Group	

3.1.1.1 802.11n Radio Transmitter

Enable 802.11n Radio Transmitter	1
Name Prefix	SonicPointN
Country Code	840
802.11n Radio Mode	2.4Ghz 11Mbps - 802.11b
802.11n Channel	AutoChannel
802.11n SSID	sonicwall-A94C
Authentication Type	WEP - Both (Open System & Shared Key)
WEP Key Type	None, Alphanumeric
Default Key	1
Key 1	
Key 2	
Key 3	
Key 4	
Hide SSID in Beacon	0
Schedule IDS Scan	
Data Rate	0
Transmit Power	0
Antenna Diversity	0
Beacon Interval (msec)	100
DTIM Interval	1
Fragementation Threshold (bytes)	2346
RTS Threshold (bytes)	2346
Maximum Client Associates	32
Preample Length	1
CCK OFDM Power Delta	10
Protection Mode	0
Protection Rate	1
Protection Type	0
Enable Short Slot Time	0
Allow Only 802.11N Clients to Conect	0

4. Firewall

4.1 Access Rules

4.1.1 'LAN' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
1	LAN	LAN	Any	All LAN Management IP	Ping	Allow	Yes
2	LAN	LAN	Any	All LAN Management IP	SSH Management	Allow	Yes
3	LAN	LAN	Any	All LAN Management IP	HTTPS Management	Allow	Yes
4	LAN	LAN	Any	All LAN Management IP	HTTP Management	Allow	Yes
5	LAN	LAN	Any	Any	Any	Allow	Yes

Details for Access Rule # 1

Source	Any
Destination	All LAN Management IP
Service	Ping
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 2

Source	Any
Destination	All LAN Management IP
Service	SSH Management
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 3

Source	Any
Destination	All LAN Management IP
Service	HTTPS Management
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 4

Source	Any

Destination	All LAN Management IP
Service	HTTP Management
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 5

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added Interface Trust rule

4.1.2 'LAN' to 'WAN'

#	From	To	Source	Destination	Service	Action	Enabled
6	LAN	WAN	Any	Any	Any	Allow	Yes

Details for Access Rule # 6

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.3 'LAN' to 'DMZ'

#	From	To	Source	Destination	Service	Action	Enabled
7	LAN	DMZ	Any	Any	Any	Allow	Yes

Details for Access Rule # 7

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.4 'LAN' to 'VPN'

#	From	To	Source	Destination	Service	Action	Enabled
8	LAN	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No
9	LAN	VPN	WLAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 8

Source	WAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WAN GroupVPN

Details for Access Rule # 9

Source	WLAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WLAN GroupVPN

4.1.5 'LAN' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
10	LAN	MULTICAST	Any	Any	Any	Allow	Yes

Details for Access Rule # 10

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.6 'LAN' to 'WLAN'

#	From	To	Source	Destination	Service	Action	Enabled
11	LAN	WLAN	Any	Any	Any	Allow	Yes

Details for Access Rule # 11

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.7 'WAN' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
12	WAN	LAN	Any	Any	Any	Deny	Yes

Details for Access Rule # 12

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny

Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.8 'WAN' to 'WAN'

#	From	To	Source	Destination	Service	Action	Enabled
13	WAN	WAN	Any	All WAN Management IP	Ping	Allow	Yes
14	WAN	WAN	Any	All WAN Management IP	HTTPS Management	Allow	Yes
15	WAN	WAN	Any	All WAN Management IP	HTTP Management	Allow	Yes

Details for Access Rule # 13

Source	Any
Destination	All WAN Management IP
Service	Ping
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 14

Source	Any
Destination	All WAN Management IP
Service	HTTPS Management
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 15

Source	Any
Destination	All WAN Management IP
Service	HTTP Management
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes

TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

4.1.9 'WAN' to 'DMZ'

#	From	To	Source	Destination	Service	Action	Enabled
16	WAN	DMZ	Any	Any	Any	Deny	Yes

Details for Access Rule # 16

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.10 'WAN' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
17	WAN	MULTICAST	Any	Any	Any	Deny	Yes

Details for Access Rule # 17

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.11 'WAN' to 'WLAN'

#	From	To	Source	Destination	Service	Action	Enabled
18	WAN	WLAN	Any	Any	Any	Deny	Yes

Details for Access Rule # 18

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.12 'DMZ' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
19	DMZ	LAN	Any	Any	Any	Deny	Yes

Details for Access Rule # 19

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.13 'DMZ' to 'WAN'

#	From	To	Source	Destination	Service	Action	Enabled
20	DMZ	WAN	Any	Any	Any	Allow	Yes

Details for Access Rule # 20

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None

802.1p Marking Action	None

4.1.14 'DMZ' to 'DMZ'

#	From	To	Source	Destination	Service	Action	Enabled
21	DMZ	DMZ	Any	Any	Any	Allow	Yes

Details for Access Rule # 21

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added Interface Trust rule

4.1.15 'DMZ' to 'VPN'

#	From	To	Source	Destination	Service	Action	Enabled
22	DMZ	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No
23	DMZ	VPN	WLAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 22

Source	WAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WAN GroupVPN

Details for Access Rule # 23

Source	WLAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow

Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WLAN GroupVPN

4.1.16 'DMZ' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
24	DMZ	MULTICAST	Any	Any	Any	Allow	Yes

Details for Access Rule # 24

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.17 'DMZ' to 'WLAN'

#	From	To	Source	Destination	Service	Action	Enabled
25	DMZ	WLAN	Any	Any	Any	Deny	Yes

Details for Access Rule # 25

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.18 'VPN' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
26	VPN	LAN	Any	All LAN Management IP	SNMP	Allow	Yes
27	VPN	LAN	Any	All LAN Management IP	Ping	Allow	Yes
28	VPN	LAN	Any	WAN RemoteAccess Networks	Any	Allow	No
29	VPN	LAN	Any	WLAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 26

Source	Any
Destination	All LAN Management IP
Service	SNMP
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	No
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 27

Source	Any
Destination	All LAN Management IP
Service	Ping
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	No
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto-added management rule

Details for Access Rule # 28

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 29

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

4.1.19 'VPN' to 'WAN'

#	From	To	Source	Destination	Service	Action	Enabled
30	VPN	WAN	Any	WAN RemoteAccess Networks	Any	Allow	No
31	VPN	WAN	Any	WLAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 30

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 31

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

4.1.20 'VPN' to 'DMZ'

#	From	To	Source	Destination	Service	Action	Enabled
32	VPN	DMZ	Any	WAN RemoteAccess Networks	Any	Allow	No
33	VPN	DMZ	Any	WLAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 32

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 33

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

4.1.21 'VPN' to 'VPN'

#	From	To	Source	Destination	Service	Action	Enabled
34	VPN	VPN	Any	WAN RemoteAccess Networks	Any	Allow	No
35	VPN	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No
36	VPN	VPN	Any	WLAN RemoteAccess Networks	Any	Allow	No
37	VPN	VPN	WLAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 34

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any

User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 35

Source	WAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WAN GroupVPN

Details for Access Rule # 36

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

Details for Access Rule # 37

Source	WLAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WLAN GroupVPN

4.1.22 'VPN' to 'SSLVPN'

#	From	To	Source	Destination	Service	Action	Enabled
38	VPN	SSLVPN	Any	WAN RemoteAccess Networks	Any	Allow	No
39	VPN	SSLVPN	Any	WLAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 38

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 39

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

4.1.23 'VPN' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
40	VPN	MULTICAST	Any	WAN RemoteAccess Networks	Any	Allow	No
41	VPN	MULTICAST	Any	WLAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 40

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No

Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 41

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

4.1.24 'VPN' to 'WLAN'

#	From	To	Source	Destination	Service	Action	Enabled
42	VPN	WLAN	Any	WAN RemoteAccess Networks	Any	Allow	No
43	VPN	WLAN	Any	WLAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 42

Source	Any
Destination	WAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WAN GroupVPN

Details for Access Rule # 43

Source	Any
Destination	WLAN RemoteAccess Networks
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes

Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for inbound VPN - WLAN GroupVPN

4.1.25 'SSLVPN' to 'VPN'

#	From	To	Source	Destination	Service	Action	Enabled
44	SSLVPN	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No
45	SSLVPN	VPN	WLAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 44

Source	WAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WAN GroupVPN

Details for Access Rule # 45

Source	WLAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WLAN GroupVPN

4.1.26 'WLAN' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
46	WLAN	LAN	Any	Any	Any	Deny	Yes

Details for Access Rule # 46

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.27 'WLAN' to 'WAN'

#	From	To	Source	Destination	Service	Action	Enabled
47	WLAN	WAN	Any	Any	Any	Allow	Yes

Details for Access Rule # 47

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.28 'WLAN' to 'DMZ'

#	From	To	Source	Destination	Service	Action	Enabled
48	WLAN	DMZ	Any	Any	Any	Allow	Yes

Details for Access Rule # 48

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	Yes
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.1.29 'WLAN' to 'VPN'

#	From	To	Source	Destination	Service	Action	Enabled
49	WLAN	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No
50	WLAN	VPN	WLAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 49

Source	WAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WAN GroupVPN

Details for Access Rule # 50

Source	WLAN RemoteAccess Networks
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Allow
Enabled	No
Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	15 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None
Comment	Auto added for outbound VPN - WLAN GroupVPN

4.1.30 'WLAN' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
51	WLAN	MULTICAST	Any	Any	Any	Deny	Yes

Details for Access Rule # 51

Source	Any
Destination	Any
Service	Any
User	All
Schedule	Always on
Action	Deny
Enabled	Yes

Enable Logging	Yes
Allow Fragmented Packets	Yes
TCP Connection Inactivity Timeout	5 minutes
UDP Connection Inactivity Timeout	30 seconds
Number of connections allowed	100% of maximum connections
DSCP Marking Action	None
802.1p Marking Action	None

4.2 App Rules

App Rules Global Settings

Enable App Rules	off
Global Log Redundancy Filter (seconds)	0

4.2.1 App Rules Policies

4.3 Services

4.3.1 Service Groups

#	Name	Members
1	NT Domain Login	LDAP, Kerberos, NetBios, NT Domain Login Port 1025, DCE EndPoint
2	SonicWALL SSO Agents	
3	SonicWALL TS Agents	
4	Terminal Services	Terminal Services TCP, Terminal Services UDP
5	Citrix	Citrix TCP, Citrix TCP (Session Reliability), Citrix UDP
6	IRC (Chat)	IRC (Chat) 194, IRC (Chat) 6666-6670, IRC (Chat) 7000
7	DNS (Name Service)	DNS (Name Service) TCP, DNS (Name Service) UDP
8	FTP (All)	FTP Data, FTP Control
9	IKE	IKE (Key Exchange), IKE (Traversal)
10	ICMP	Echo Reply, Destination Unreachable, Source Quench, Redirect, Echo, Router Advertisement, Router Solicitation, Time Exceeded
11	Ping	Ping 0, Ping 8
12	Kerberos	Kerberos TCP, Kerberos UDP
13	NetBios	NetBios NS TCP, NetBios NS UDP, NetBios DGM TCP, NetBios DGM UDP, NetBios SSN TCP, NetBios SSN UDP, SMB
14	NFS	NFS TCP, NFS UDP
15	Syslog	Syslog TCP, Syslog UDP
16	VOIP	H323 Call Signaling, H323 Gatekeeper Discovery, H323 Gatekeeper RAS, MGCP TCP, MGCP UDP, SIP, Skinny, T120 (Whiteboard+A43)
17	PC Anywhere	PC Anywhere TCP, PC Anywhere UDP
18	Timbuktu	Timbuktu TCP 407, Timbuktu UDP 407, Timbuktu TCP 1417-1420, Timbuktu UDP 1419
19	Streaming media	RTSP, PNA, MMS, MSN
20	RTSP	RTSP TCP, RTSP UDP
21	MMS	MMS TCP, MMS UDP
22	MSN	MSN TCP, MSN UDP
23	Yahoo Messenger	Yahoo Messenger TCP, Yahoo Messenger UDP
24	VNC	VNC 5500, VNC 5800, VNC 5900
25	P2P Services	Edonkey, WinMX, Kazaa / FastTrack, iMesh, Direct Connect, BearShare
26	Edonkey	Edonkey TCP, Edonkey UDP
27	WinMX	WinMX TCP 6699, WinMX TCP 7729-7735, WinMX UDP 6257
28	IGMP	Membership Query, V2 Membership Report, Leave Group, V3 Membership Report
29	Multicast RTP	
30	ShoreTel	ShoreTel Call Control, ShoreTel RTP, ShoreTel IP Phone Control 2427, ShoreTel IP Phone Control 2727

31	Tivo Services	Tivo TCP Beacon, Tivo UDP Beacon, Tivo TCP Data, Tivo TCP Desktop (8101/8102), Tivo TCP Desktop (8200)

4.3.2 Services

#	Name	Protocol	Port Start	Port End
1	HTTP	6	80	80
2	HTTP Management	6	80	80
3	HTTPS	6	443	443
4	HTTPS Management	6	443	443
5	IDENT	6	113	113
6	IMAP3	6	220	220
7	IMAP4	6	143	143
8	ISAKMP	17	500	500
9	LDAP	6	389	389
10	LDAPS	6	636	636
11	LPR (Unix Printer)	6	515	515
12	MS SQL	6	1433	1433
13	NNTP (News)	6	119	119
14	NTP	17	123	123
15	POP3 (Retrieve E-Mail)	6	110	110
16	Terminal Services TCP	6	3389	3389
17	Terminal Services UDP	17	3389	3389
18	PPTP	6	1723	1723
19	SMTP (Send E-Mail)	6	25	25
20	SNMP	17	161	162
21	SQL*Net	6	1521	1521
22	SSH	6	22	22
23	Telnet	6	23	23
24	TFTP	17	69	69
25	Citrix TCP	6	1494	1494
26	Citrix TCP (Session Reliability)	6	2598	2598
27	Citrix UDP	17	1604	1604
28	IRC (Chat) 194	6	194	194
29	IRC (Chat) 6666-6670	6	6666	6670
30	IRC (Chat) 7000	6	7000	7000
31	DNS (Name Service) TCP	6	53	53
32	DNS (Name Service) UDP	17	53	53
33	Enhanced TV	6	9000	9000
34	ESP (IPSec)	50	1	1
35	FTP	6	21	21
36	FTP Data	6	20	20
37	FTP Control	6	21	21
38	Gopher	6	70	70
39	IKE (Key Exchange)	17	500	500
40	IKE (Traversal)	17	4500	4500
41	Lotus Notes	6	1352	1352
42	Echo Reply	1	0	0
43	Destination Unreachable	1	3	3
44	Source Quench	1	4	4
45	Redirect	1	5	5
46	Echo	1	8	8
47	Router Advertisement	1	9	9
48	Router Solicitation	1	10	10
49	Time Exceeded	1	11	11
50	Ping 0	1	0	0
51	Ping 8	1	8	8
52	Kerberos TCP	6	88	88
53	Kerberos UDP	17	88	88
54	NetBios NS TCP	6	137	137
55	NetBios NS UDP	17	137	137
56	NetBios DGM TCP	6	138	138
57	NetBios DGM UDP	17	138	138

58	NetBios SSN TCP	6	139	139
59	NetBios SSN UDP	17	139	139
60	SMB	6	445	445
61	NFS TCP	6	2049	2049
62	NFS UDP	17	2049	2049
63	Syslog TCP	6	514	514
64	Syslog UDP	17	514	514
65	H323 Call Signaling	6	1720	1720
66	H323 Gatekeeper Discovery	17	1718	1718
67	H323 Gatekeeper RAS	17	1719	1719
68	MGCP TCP	6	2428	2428
69	MGCP UDP	17	2427	2427
70	SIP	17	5060	5061
71	Skinny	6	2000	2000
72	T120 (Whiteboard+A43)	6	1503	1503
73	PC Anywhere TCP	6	5631	5631
74	PC Anywhere UDP	17	5632	5632
75	Timbuktu TCP 407	6	407	407
76	Timbuktu UDP 407	17	407	407
77	Timbuktu TCP 1417-1420	6	1417	1420
78	Timbuktu UDP 1419	17	1419	1419
79	RTSP TCP	6	554	554
80	RTSP UDP	17	554	554
81	PNA	6	7070	7070
82	MMS TCP	6	1755	1755
83	MMS UDP	17	1755	1755
84	MSN TCP	6	1863	1863
85	MSN UDP	17	1863	1863
86	Squid	6	3128	3128
87	Yahoo Messenger TCP	6	5050	5050
88	Yahoo Messenger UDP	17	5050	5050
89	VNC 5500	6	5500	5500
90	VNC 5800	6	5800	5800
91	VNC 5900	6	5900	5900
92	Remotely Anywhere	6	2000	2000
93	Remotely Possible	6	799	799
94	Quake	17	27910	27910
95	cu-seeme	17	24032	24032
96	Edonkey TCP	6	4661	4662
97	Edonkey UDP	17	4665	4665
98	WinMX TCP 6699	6	6699	6699
99	WinMX TCP 7729-7735	6	7729	7735
100	WinMX UDP 6257	17	6257	6257
101	Kazaa / FastTrack	6	1214	1214
102	iMesh	6	4000	5000
103	Direct Connect	6	411	412
104	BearShare	6	6346	6349
105	ZebTelnet	6	2601	2620
106	Membership Query	2	17	17
107	V2 Membership Report	2	22	22
108	Leave Group	2	23	23
109	V3 Membership Report	2	34	34
110	GMS HTTPS	6	3003	3003
111	Radius	17	1812	1812
112	GSCTrace	6	59162	59162
113	SSH Management	6	22	22
114	NT Domain Login Port 1025	6	1025	1025
115	DCE EndPoint	6	135	135
116	External Guest Authentication	6	4043	4043
117	ShoreTel Call Control	17	5440	5446
118	ShoreTel RTP	17	5004	5004
119	ShoreTel IP Phone Control 2427	17	2427	2427
120	ShoreTel IP Phone Control 2727	17	2727	2727
121	Tivo TCP Beacon	6	2190	2190
122	Tivo UDP Beacon	17	2190	2190

123	Tivo TCP Data	6	8080	8089
124	Tivo TCP Desktop (8101/8102)	6	8101	8102
125	Tivo TCP Desktop (8200)	6	8200	8200
126	IPcomp	108	1	1
127	Apple Bonjour	17	5353	5353
128	SMTP (Anti-Spam Inbound Port)	6	25	25
129	SSLVPN	6	4433	4433
130	6over4	41	1	1

5. Firewall Settings

5.1 Advanced

Enable Stealth Mode	off
Randomize IP ID	off
Decrement IP TTL for forwarding traffic	off
Never generate ICMP Time-Exceeded packets	off
Enable support for Oracle (SQLNet)	on
Enable Support for Windows Messenger	off
Enable RTSP Transformations	on
Drop source routed IP packets	on
Disable Application Firewall, AS, GAV and IPS	off
Force inbound/outbound FTP to use port 20	off
Enable IP header checksum enforcement	off
Enable UDP checksum enforcement	off
Default UDP connection timeout (seconds)	30

5.2 Flood Protection

TCP Settings

Enforce strict TCP compliance	off
Enable TCP handshake enforcement	off
Enable TCP checksum enforcement	off
TCP Handshake Timeout (seconds)	30
Default TCP connection timeout (minutes)	15
Maximum segment lifetime (seconds)	8

Layer 3 SYN Flood Protection - SYN Proxy

SYN Flood protection mode	Watch and report possible SYN Floods
SYN Attack threshold from gathered statistics	300
Attack threshold (connection attempts / second)	300
All LAN/DMZ servers support the TCP SACK option	off
Limit MSS sent to WAN clients	off
Maximum TCP MSS set to WAN clients	1460
Always log SYN packets received	off

Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

Threshold for SYN/RST/FIN flood blacklisting	1000
Enable SYN/RST/FIN flood blacklisting on all interfaces	off
Never blacklist WAN machines	off
Always allow SonicWall management traffic	off

UDP Settings

Default UDP Connection Timeout (seconds)	30

UDP Flood Protection

Enable UDP Flood Protection	
UDP Flood Attack Threshold (UDP Packets / Sec)	
UDP Flood Attack Blocking Time (Sec)	
UDP Flood Attack Protected Destination List	

ICMP Flood Protection

Enable ICMP Flood Protection	
ICMP Flood Attack Threshold (ICMP Packets / Sec)	
ICMP Flood Attack Blocking Time (Sec)	
ICMP Flood Attack Protected Destination List	

5.3 Multicast

Multicast Snooping

Enable Multicast	off
Require IGMP Membership for multicast data forwarding	on
Multicast state table entry timeout (minutes)	5

Multicast Policies

	Enable reception for the following multicast addresses

5.4 Qos Mapping

802.1p Class Of Service	To DSCP	From DSCP Range
0 - Best Effort	0 - Best effort/Default	0-7
1 - Background	8 - Class 1	8-15
2 - Spare	16 - Class 2	16-23
3 - Excellent Effort	24 - Class 3	24-31
4 - Controlled load	32 - Class 4	32-39
5 - Video (<100ms latency)	40 - Express Forwarding	40-47
6 - Voice (<10ms latency)	48 - Control	48-55
7 - Network Control	56 - Control	56-63

5.5 SSL Control

Enable SSL Control	
If an SSL policy violation is detected	Block the connection and log the event
Enable Blacklist	On
Enable Whitelist	On
Detect expired certificates	Off
Detect SSLv2	Off
Detect Self-Signed Certificates	On
Detect Certificates signed by an Untrusted CA	On
Detect Weak Ciphers (<64bits)	Off

6. DPI-SSL

6.1 Client SSL

Enable SSL Client Inspection:off

6.2 Server SSL

Enable SSL Server Inspection:off

7. VoIP

Enable consistent NAT	off

7.1 SIP Settings

Enable SIP support	off
Permit non-SIP packets on signaling port	off
SIP signaling inactivity time out (seconds)	1800
SIP media inactivity time out (seconds)	120
Additional SIP signaling port (UDP)	0

7.2 H.323 Settings

Enable H.232 Transformations	off
Enable LDAP ILS Support	off
Only accept incoming calls from Gatekeeper	off
H.323 Signaling/Media inactivity time out	300
Default WAN/DMZ Gatekeeper IP Address	0.0.0.0

8. Anti-Spam

8.1 Settings

Anti-Spam Global Settings

Enable Anti-Spam Service	off

9. VPN

9.1 Settings

VPN Global Settings

Enable VPN	on
Unique Firewall Identifier	0017C50FA94C

9.2 VPN Policies

9.2.1 WAN GroupVPN

Disabled	on
IPSec Primary Gateway	0.0.0.0
IPSec Secondary Gateway	0.0.0.0
Authentication Method	IKE using 3rd Party Certificates
Shared Secret	XXXXXXXX
Peer IKE ID	Domain Name: GroupVPN

Local Networks

Local network obtains IP addresses using DHCP through this VPN Tunnel	off
Any address	off

Destination Networks

Use this VPN Tunnel as default route for all Internet traffic	off
Destination network obtains IP addresses using DHCP through this VPN Tunnel	off

IKE (Phase 1) Proposal

Exchange	Aggressive Mode
Diffie-Hellmann Group	2
Encryption	3DES
Authentication	SHA1
Life Time (seconds)	28800

IPSec (Phase 2) Proposal

Incoming SPI	on
Outgoing SPI	on
Protocol	ESP (IP50)
Encryption	3DES
Authentication	SHA1
Encryption Key	XXXXXXXX
Authentication Key	XXXXXXXX
Enable Perfect Forward Secrecy	off
Diffie-Hellmann Group	1
Life Time (seconds)	28800

Advanced Settings

Enable Keep Alive	off
Suppress automatic Access Rules creation for VPN Policy	off
Require Authentication of VPN Clients via XAUTH	on
User Group for XAUTH users	Trusted Users
Enable Windows Networking (NetBIOS) Broadcast	off
Enable Multicast	off
Apply NAT Policies	off
Translated Local Network	
Translated Remote NetworkP	
Management via this SA by HTTP	off
Management via this SA by HTTPS	off
Management via this SA by SSH	off
Default Gateway	0.0.0.0
Allow Unauthenticated VPN Client Access	

Client Settings

Cache XAUTH User Name and Password on Client	off
Virtual Adapter Settings	None
Allow Connections to	All Secured Gateways
Set Default Route at this Gateway	off
Require Global Security Client for this Connection	off

Use Default Key for Simple Client Provisioning

9.2.2 WLAN GroupVPN

Disabled	on
IPSec Primary Gateway	0.0.0.0
IPSec Secondary Gateway	0.0.0.0
Authentication Method	IKE using 3rd Party Certificates
Shared Secret	XXXXXXXX
Peer IKE ID	Domain Name: GroupVPN

Local Networks

Local network obtains IP addresses using DHCP through this VPN Tunnel	off
Any address	off

Destination Networks

Use this VPN Tunnel as default route for all Internet traffic	on
Destination network obtains IP addresses using DHCP through this VPN Tunnel	off

IKE (Phase 1) Proposal

Exchange	Aggressive Mode
Diffie-Hellmann Group	2
Encryption	3DES
Authentication	SHA1
Life Time (seconds)	28800

IPSec (Phase 2) Proposal

Incoming SPI	on
Outgoing SPI	on
Protocol	ESP (IP50)
Encryption	3DES
Authentication	SHA1
Encryption Key	XXXXXXXX
Authentication Key	XXXXXXXX
Enable Perfect Forward Secrecy	off
Diffie-Hellmann Group	1
Life Time (seconds)	28800

Advanced Settings

Enable Keep Alive	off
Suppress automatic Access Rules creation for VPN Policy	off
Require Authentication of VPN Clients via XAUTH	on
User Group for XAUTH users	Trusted Users
Enable Windows Networking (NetBIOS) Broadcast	off
Enable Multicast	off
Apply NAT Policies	off
Translated Local Network	
Translated Remote NetworkP	
Management via this SA by HTTP	on
Management via this SA by HTTPS	on
Management via this SA by SSH	on
Default Gateway	0.0.0.0
Allow Unauthenticated VPN Client Access	

Client Settings

Cache XAUTH User Name and Password on Client	on
Virtual Adapter Settings	None
Allow Connections to	Split Tunnels
Set Default Route at this Gateway	on
Require Global Security Client for this Connection	off
Use Default Key for Simple Client Provisioning	

9.3 Advanced

Enable IKE Dead Peer Detection	on
Dead Peer Detection Interval (seconds)	60
Failure Trigger Level (missed heartbeats)	3
Enable Dead Peer Detection for Idle VPN Sessions	off
Dead Peer Detection Interval for idle VPN sessions (seconds)	600
Enable Fragmented Packet Handling	on
Ignore DF (Don't Fragment) Bit	on
Enable NAT Traversal	on
Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address	on
Preserve IKE Port for Pass Through Connections	off
Enable OCSP Checking	off
Send VPN Tunnel Traps only when tunnel status changes	off
Use RADIUS in MSCHAP mode for XAUTH	on
Use RADIUS in MSCHAPv2 mode for XAUTH	off
Send IKEv2 Cookie Notify	off
IKEv2 Dynamic Client Proposal: DH Group	2
IKEv2 Dynamic Client Proposal: Encryption	3DES
IKEv2 Dynamic Client Proposal: Authentication	SHA1

9.4 DHCP over VPN

9.4.1 Central Gateway

DHCP Relay

Use Internal DHCP Server	off
For Global VPN Client	off
For Remote Firewall	off

Send DHCP requests to the server addresses listed below

Relay IP Address (Optional)	0.0.0.0

9.5 L2TP Server

Enable L2TP Server	off

10. SSL VPN

10.1 Server Settings

SSL VPN Server Settings

SSL VPN Port	4433
Certificate Selection	Use Selfsigned Certificate
Enable Server Cipher Preference	off

10.2 Portal Settings

Portal Settings

Portal Site Title	
Portal Banner Title	
Home Page Message	
Login Message	

Portal Logo Settings

Use Default SonicWALL Logo	off
Customized Logo	/VirtualOffice.gif

10.3 Client Settings

SSLVPN Client Address Range

Interface	
NetExtender Start IP	0.0.0.0
NetExtender End IP	0.0.0.0
DNS Server 1	0.0.0.0
DNS Server 2	0.0.0.0
DNS Domain	
User Domain	
WINS Server 1	0.0.0.0
WINS Server 2	0.0.0.0

10.4 Client Routes

SSLVPN Client Address Range

Tunnel All Mode	Disabled

Name	Address Detail	Type	Zone

11. Virtual Assist

General Setting

Assistance Code	
Enable Support without Invitation	off
Disclaimer	
Customer Access Link	
Display Virtual Assist link from Portal Login	off

Notification Settings

Technician E-mail List	
Subject of Invitation	
Invitation Message	

Request Settings

Maximum Requests	10
Limit Message	
Maximum Requests From One IP	0
Pending Request Expired	0

Restriction Settings

12. Users

12.1 Settings

User Login Settings

Authentication method for login	Local Users
Single-sign-on method	None
Show authentication page for (minutes)	1
Case-sensitive user names	on
Enforce login uniqueness	off
Redirect users from HTTPS to HTTP on completion of login	on

User Session Settings

Inactivity timeout (minutes)	15
Enable login session limit	
Login session limit (minutes)	30
Show user login status window	
User's login status window sends heartbeat every (seconds)	120
Enable disconnected user detection	
Timeout on heartbeat from user's login status window (minutes)	10

Other Global User Settings

Allow these HTTP URLs to bypass user authentication in access rules

Acceptable Use Policy

Display on login from	Trusted Zones on	WAN Zone off	Public Zones on	Wireless Zones off	VPN Zone off
Window size (pixels)	460 x 310				
Enable scroll bars on the window					

Acceptable use policy page content

12.1.1 SonicWALL SSO Agent Settings

Authentication Agent Settings

Name or IP Address	
Port Number	
Shared Key	XXXXXXXX
Timeout (seconds)	
Retries	

12.1.2 SonicWALL SSO Agent Users

User Settings

Allow only users listed locally	off
Simple user names in local database	on
Allow limited access for non-domain users	off
Mechanism for setting user group memberships	Use LDAP to retrieve user group information
Polling rate (minutes)	5
Hold time after failure (minutes)	1

12.2 Local Groups

Local Groups	Bypass Filters	Guest Services	Admin	Members	Comment
Everyone					
Guest Services		on			
Trusted Users					
Content Filtering Bypass	on				
Limited Administrators			Ltd.		
SonicWALL Administrators			Full		
SonicWALL Read-Only Admins			Rd-Only		
SSLVPN Services					

12.3 Guest Services

Global Guest Settings

Show guest login status window with logout button	on

Guest Profiles	Bypass Filters	Guest Services	Admin	Comment
Default				Auto-Generated

13. High Availability

13.1 Settings

High Availability Settings	
Enable High Availability	off

SonicWALL Address Settings	
Primary SonicWALL Serial Number	0017C50FA94C
Backup SonicWALL Serial Number	000000000000

13.2 Advanced

High Availability Advanced Settings	
Enable Stateful Synchronization	off
Enable Active/Active UTM	off
Enable Preempt Mode	off
Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware	off
Enable Virtual MAC	off
Heartbeat Interval (millseconds)	5000
Failover Trigger Level (missed heartbeats)	5
Probe Interval (seconds)	20
Election Delay Time (seconds)	3
Dynamic Route Hold-Down Time (seconds)	45
Include Certificates/Keys	on

13.3 High Availability Monitoring Settings

Interface	Primary IP	Backup IP	Probe IP	Monitoring Physical/Link	Logical/Probe	Management	Override Virtual MAC
X0				on			
X1				on			

14. Security Services

14.1 Summary

Security Services Settings	
Maximum Security (Recommended)	
Reduce Anti-Virus and E-Mail Filter traffic for ISDN connections	off
Drop all packets while IPS, GAV and Anti-Spyware database is reloading	off
HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware (sec)	86400

Signature Downloads Through a Proxy Server	
Download Signatures through a Proxy Server	off
Proxy Server Name or IP Address	
Proxy Server Port	0
This Proxy Server requires Authentication	off

14.2 Content Filter

Content Filter Type
Websense Enterprise

Websense Enterprise Settings	
Server Host Name or IP Address	test.sbi_enforceSafeSearch
Server Port	15868
User Name	schimpanse
If Server is unavailable for (secs)	5
	Block traffic to all Web sites

URL Cache	
Cache Size (KB)	50

Restrict Web Features	
ActiveX	off
Java	off
Cookies	off
Access to HTTP Proxy Servers	off

CFS Exclusion for the Administrator	
Do not bypass CFS blocking for the Administrator	off

CFS Exclusion List	
Enable CFS Exclusion List	off
Exclude from	CFS and user authentication in access rules

14.3 Client AV Enforcement

Administration	
Disable policing from Trusted to Public	off
Days before forcing update	5
Low Risk	off
Medium Risk	on
High Risk	on
Client Anti-Virus Enforcement	Enforce Client Anti-Virus policies for all computers

14.4 Gateway Antivirus

Gateway Anti-Virus Global Settings

Enable Gateway Anti-Virus	off

Gateway AV Settings

Disable SMTP Responses	off
Disable detection of EICAR test virus	on
Enable HTTP Byte-Range requests with Gateway AV	on
Enable FTP 'REST' requests with Gateway AV	on
Do not scan parts of files with high compression ratios	on
Block files with multiple levels of zip/gzip compression	
Enable detection-only mode	

HTTP Clientless Notification

Enable HTTP Clientless Notification Alerts	on

Message to Display when Blocking

This request is blocked by the SonicWALL Gateway Anti-Virus Service.

Protocols	HTTP	FTP	IMAP	SMTP	POP3	CIFS/Netbios	TCP Stream
Enable Inbound Inspection	on	on	on	on	on	off	off
Enable Outbound Inspection	off	off		off			off
Restrict Transfer of password-protected ZIP files	off	off	on	on	on	off	
Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)	off	off	on	on	on	off	
Restrict Transfer of packed executable files (UPX, FSG, etc.)	off	off	on	on	on	off	

14.5 Intrusion Prevention

IPS Global Settings

Enable IPS	off

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Priority Attacks	off	off	0
Medium Priority Attacks	off	off	0
Low Priority Attacks	off	off	60

IPS Network Services

Enable IP Reassembly

IPS Exclusion List

Enable IPS Exclusion List	off

14.6 Anti-Spyware

Anti-Spyware Global Settings

Enable Anti-Spyware	off

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Danger Level Spyware	off	off	0
Medium Danger Level Spyware	off	off	0
Low Danger Level Spyware	off	off	0

Protocols	HTTP	FTP	IMAP	SMTP	POP3
Enable Inbound Inspection	on	on	on	on	on
	Enable Inspection of Outbound Spyware Communication				

14.7 RBL Filter

Real-time Black List Settings

Enable Real-time Black List Blocking	off
RBL DNS Servers	Inherit Settings from WAN Zone

Real-time Black List Services		RBL Blocked Responses
sbl-xbl.spamhaus.org	on	
		127.0.0.2 - Open Relay
		127.0.0.3 - Dialup Spam Source
		127.0.0.4 - Spam Source
		127.0.0.5 - Smart Host
		127.0.0.6 - Spamware
		127.0.0.7 - Bad List Server
		127.0.0.8 - Insecure Script
		127.0.0.9 - Open Proxy Server
dnsbl.sorbs.net	on	
		127.0.0.2 - Open Relay
		127.0.0.3 - Dialup Spam Source
		127.0.0.4 - Spam Source
		127.0.0.5 - Smart Host
		127.0.0.6 - Spamware
		127.0.0.7 - Bad List Server
		127.0.0.8 - Insecure Script
		127.0.0.9 - Open Proxy Server

14.8 GeoIP Filter

General

Block connections to/from selected countries	Firewall Rule-based
Enable Logging	

Geo-IP Exclusion Object

15. Log

15.1 Categories

Log Severity/Priority

Logging Level	Debug	Log Redundancy Filter (seconds)	60
Alert Level	Alert	Alert Redundancy Filter (seconds)	900

Category	Description	Log	Alerts	Syslog
802.11b Management	Legacy category	off	off	off
Advanced Routing	ARS Logging	on	off	on
Advanced Switching	Advanced Switching Activity	on	off	on
Anti-Spam Service	Anti-Spam Service	on	on	on
Application Firewall	Application Firewall Activity	on	off	on
Attacks	Legacy category	on	on	on
Authenticated Access	Adminstrator, user, and guest account activity	on	off	on
BOOTP	BOOTP activity	off	off	off
Blocked Java Etc	Legacy category	on	off	on
Blocked Web Sites	Legacy category	on	off	on
Crypto Test	Crypto algorithm and hardware testing	off	off	off
DDNS	Dynamic DNS activity	off	off	off
DHCP Client	DHCP client protocol activity	on	off	on
DHCP Relay	DHCP central and remote gateway activity	off	off	off
Denied LAN IP	Legacy category	off	off	off
Dropped ICMP	Legacy category	on	off	on
Dropped TCP	Legacy category	on	off	on
Dropped UDP	Legacy category	on	off	on
Dynamic Address Objects	MAC/FQDN Address Object binding status messages	off	off	off
Firewall Event	Internal firewall activity	on	off	on
Firewall Hardware	Firewall hardware error conditions	on	off	on
Firewall Logging	Logging events and errors	on	off	on
Firewall Rule	Firewall rule modifications	off	off	off
GMS	GMS status event	off	off	off
High Availability	High Availability activity	off	off	off
IPcomp	IP compression activity	on	off	on
Intrusion Prevention	Logged events	on	off	on
L2TP Client	L2TP client activity	off	off	off
L2TP Server	L2TP server activity	off	off	off
Multicast	Multicast IGMP activity	off	off	off
Network	Network ARP, fragmentation, MTU activity	off	off	off
Network Access	Network and firewall protocol access activity	off	off	off
Network Debug	Legacy category	off	off	off
Network Traffic	Network traffic reporting events	off	off	on
PPP	Generic PPP activity	on	off	on
PPPoE	PPPoE activity	on	off	on
PPTP	PPTP activity	off	off	off
RBL	Real-time Black List activity	on	off	on
RF Monitoring	WLAN Radio Frequency Threat monitoring	on	off	on
RIP	RIP activity	off	off	off
Remote Authentication	RADIUS/LDAP server activity	off	off	off
SSO Agent Authentication	SonicWALL SSO agent user authentication activity	on	off	on
Security Services	Security services activity	on	off	on
SonicPoint	SonicPoint activity	on	off	on
System Errors	Legacy category	on	on	on
System Maintenance	Legacy category	on	off	on
User Activity	Legacy category	on	off	on
VOIP	VOIP H.323/RAS, H.323/H.225, H.323/H.245, activity	off	off	off
VPN	VPN activity	off	off	off
VPN Client	VPN Client activity	on	off	on
VPN IKE	VPN IKE activity	on	off	on
VPN IPSec	VPN IPSec activity	on	off	on
VPN PKI	VPN PKI activity	on	off	on
VPN Tunnel Status	Legacy category	off	off	off

WAN Availability	WAN availability activity	on	off	on
Wireless	Wireless activity	on	off	on
Wlan IDS	Wlan IDS activity	off	off	off

15.2 Syslog

Syslog Settings

Syslog Facility	Local Use 0
Override Syslog Settings with ViewPoint Settings	off
Syslog Event Redundancy Filter (seconds)	60
Syslog Format	Default
Enable Event Rate Limiting	off
Enable Data Rate Limiting	off

15.3 Automation

E-mail Log Automation

Send Log to E-mail Address	
Send Alerts to E-mail Address	
Send Log	When Full

Mail Server Settings

Mail Server (name or IP address)	
From E-mail Address	
Authentication Method	None

Advanced

Smtp port	25

15.4 Name Resolution

Name Resolution Settings

Name Resolution Method	None

15.5 ViewPoint

ViewPoint Settings: not enabled