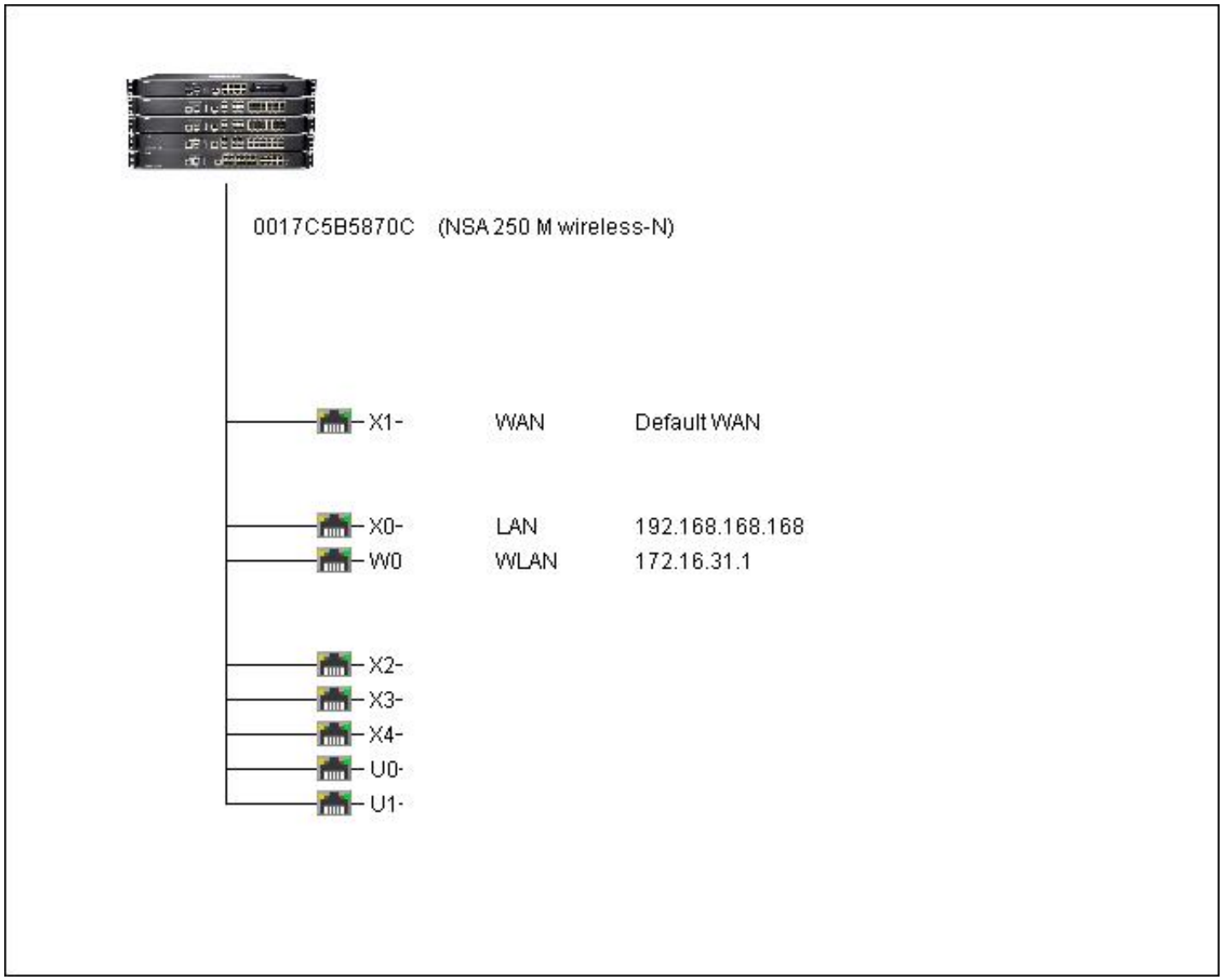
1. System



1.1 Administration

Firewall Name

Firewall Name	0017C5B5870C (NSA 250 M wireless-N)

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)	5
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	
Require PIN for front-panel access	
PIN	
LCD idle timer	

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.sonicwall.com/applications/vpnclient/

Language

Language Selection	English

1.2 Time

Timezone	Pacific Time (US & Canada) (GMT-8:00)
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
AppFlow Report Hours		
	M-T-W-TH-F-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			Static	Default WAN
X2				N/A	
X3				N/A	
X4				N/A	
W0	WLAN	172.16.31.1	255.255.255.0	Static	Default WLAN
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	Disabled
- 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:B5:87:0C
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
Comment	Default WAN
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:B5:87:0D
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:B5:87:0E
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:B5:87:0F
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:B5:87:10
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 'W0' Settings

Zone	WLAN
IP Assignment	Static
IP Address	172.16.31.1
Subnet Mask	255.255.255.0
Comment	Default WLAN
Management	
- HTTP	Disabled
- 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:B5:87:11
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 '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	Auto Negotiate
MAC Address	00:17:C5:B5:87:12
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 '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:B5:87:13
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

X1 Physical Monitoring Only

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	W0

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	"Wireless VAP 0"
2	All Interface IP	"LAN Primary IP", "WAN Primary IP", "X2 IP", "X3 IP", "X4 IP", "W0 IP", "U0 IP", "U1 IP"
3	All Rogue Access Points	
4	All Rogue Devices	
5	All SonicPoints	
6	All U0 Management IP	"U0 IP"
7	All U1 Management IP	"U1 IP"
8	All W0 Management IP	"W0 IP"
9	All WAN IP	"WAN Primary IP"
10	All X0 Management IP	
11	All X1 Management IP	
12	All X2 Management IP	"X2 IP"
13	All X3 Management IP	"X3 IP"
14	All X4 Management IP	"X4 IP"
15	Client CFS Enforcement List	
16	Default ACL Allow Group	
17	Default ACL Deny Group	
18	Default Geo-IP and Botnet Exclusion Group	"Firewalled Subnets"
19	Default SonicPoint ACL Allow Group	
20	Default SonicPoint ACL Deny Group	
21	Default Trusted Relay Agent List	
22	DMZ Interface IP	
23	DMZ Subnets	
24	Excluded from Client AV Enforcement List	
25	Excluded from Client CFS Enforcement List	
26	Firewalled Subnets	"LAN Subnets", "DMZ Subnets", "WLAN Subnets"
27	Guest Authentication Servers	
28	Kaspersky Client AV Enforcement List	
29	LAN Interface IP	"LAN Primary IP"
30	LAN Subnets	"LAN Primary Subnet"
31	McAfee Client AV Enforcement List	
32	nacDefault Device Profile for Windows	
33	nafDefault Device Profile for Windows	
34	Node License Exclusion List	
35	Public Mail Server Address Group	
36	RBL User Black List	
37	RBL User White List	
38	SSO Agents	
39	Terminal Services Agents	
40	WAN Interface IP	"WAN Primary IP"
41	WAN Subnets	"WAN Primary Subnet"
42	WLAN Interface IP	"W0 IP"
43	WLAN Subnets	"W0 Subnet"

2.5.2 Address Objects

#	Name	Address Detail	Type	Zone
1	Default Active WAN IP	0.0.0.0/255.255.255.255	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	0.0.0.0/255.255.255.255	Network	
7	U1 IP	0.0.0.0/255.255.255.255	Host	
8	U1 Subnet	0.0.0.0/255.255.255.255	Network	
9	W0 IP	172.16.31.1/255.255.255.255	Host	WLAN
10	W0 Subnet	172.16.31.0/255.255.255.0	Network	WLAN
11	WAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN
12	WLAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN
13	X0 IP	192.168.168.168/255.255.255.255	Host	LAN
14	X0 Subnet	192.168.168.0/255.255.255.0	Network	LAN
15	X1 Default Gateway	0.0.0.0/255.255.255.255	Host	WAN
16	X1 IP	0.0.0.0/255.255.255.255	Host	WAN
17	X1 Subnet	0.0.0.0/255.255.255.0	Network	WAN
18	X2 IP	0.0.0.0/255.255.255.255	Host	
19	X2 Subnet	0.0.0.0/255.255.255.255	Network	

20	X3 IP	0.0.0.0/255.255.255.255	Host
21	X3 Subnet	0.0.0.0/255.255.255.255	Network
22	X4 IP	0.0.0.0/255.255.255.255	Host
23	X4 Subnet	0.0.0.0/255.255.255.255	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
W0	WLAN	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
W0	WLAN	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 Original	Translated	Destination Original	Translated	Service Original	Translated	Src Int.	Dst. Int.	Enable	Comment
1	Any	Original	W0 IP	Original	Ping	Original	W0	W0	1	Management NAT Policy
2	Any	Original	W0 IP	Original	SSH Management	Original	W0	W0	1	Management NAT Policy
3	Any	Original	W0 IP	Original	HTTPS Management	Original	W0	W0	1	Management NAT Policy
4	Any	Original	W0 IP	Original	HTTP Management	Original	W0	W0	1	Management NAT Policy
5	Any	Original	LAN Primary IP	Original	Ping	Original	X0	X0	1	Management NAT Policy
6	Any	Original	LAN Primary IP	Original	SSH Management	Original	X0	X0	1	Management NAT Policy
7	Any	Original	LAN Primary IP	Original	HTTPS Management	Original	X0	X0	1	Management NAT Policy
8	Any	Original	LAN Primary IP	Original	HTTP Management	Original	X0	X0	1	Management NAT Policy
9	All Interface IP	WAN Primary IP	Any	Original	Any	Original	Any	X1	1	Auto-added X1 Default NAT Policy
10	Any	WAN Primary IP	Any	Original	Any	Original	W0	X1	1	Auto-added W0 outbound NAT Policy for X1 WAN
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
X0	off	off	off	off	off	off	off	off	on
X1	off	off	off	off	off	off	off	off	on
X2	off	off	off	off	off	off	off	off	on
X3	off	off	off	off	off	off	off	off	on
X4	off	off	off	off	off	off	off	off	on
W0	off	off	off	off	off	off	off	off	on

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: 172.16.31.2 - 172.16.31.254	W0	off
2	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	172.16.31.2
Range End	172.16.31.254
Lease Time (minutes)	1440
Gateway Preferences	off
Default Gateway	172.16.31.1
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	0.0.0.0
DNS Server 2	0.0.0.0
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

2.10.3 Dynamic Scope 2

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	0.0.0.0
DNS Server 2	0.0.0.0
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-870C
Authentication Type	WEP - Both (Open System & Shared Key)
WEP Key Type	None, Alphanumeric
Default Key	1
Key 1	3,dcfe358e9021be21905bb23f3bcf7060c078bd11a5e52ac9a8e5eba9964131d6
Key 2	3,a5208187365ff854069bebfee4c493a5f3e118abc77944e784d8bc5984bd98b0
Key 3	3,6d00570fe7a2de8041ed884a4793a71eddf4fd4fb2403101b910f62c520b603f
Key 4	3,6b00efe7dbeadb976e417247158b4e27783a338377b75a10b705f066093dc4f1
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

3.2 Virtual Access Point

3.2.1 Virtual Access Point Groups

#	Name	Members
1	Internal AP Group	"sonicwall"

3.2.2 Virtual Access Points

3.2.2.1 sonicwall

Profile	
VLAN ID	0
Authentication	Both
Cipher	None
Max Clients	16
SSID Suppress	0
Enable	1
Encryption Key	1

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	WLAN RemoteAccess Networks	Any	Any	Allow	No
9	LAN	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 8

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

Details for Access Rule # 9

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

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 'DMZ'

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

Details for Access Rule # 13

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

4.1.9 'WAN' to 'MULTICAST'

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

Details for Access Rule # 14

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 'WLAN'

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

Details for Access Rule # 15

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

4.1.11 'DMZ' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
16	DMZ	LAN	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

4.1.12 'DMZ' to 'WAN'

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

Details for Access Rule # 17

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

4.1.13 'DMZ' to 'DMZ'

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

Details for Access Rule # 18

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

4.1.14 'DMZ' to 'VPN'

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

Details for Access Rule # 19

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

Details for Access Rule # 20

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

4.1.15 'DMZ' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
21	DMZ	MULTICAST	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

4.1.16 'DMZ' to 'WLAN'

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

Details for Access Rule # 22

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

4.1.17 'VPN' to 'LAN'

#	From	To	Source	Destination	Service	Action	Enabled
23	VPN	LAN	Any	All LAN Management IP	Ping	Allow	Yes
24	VPN	LAN	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
25	VPN	LAN	Any	All Interface IP	SNMP	Allow	Yes

26	VPN	LAN	Any	All Interface IP	SSH Management	Allow	Yes
27	VPN	LAN	Any	All Interface IP	HTTPS Management	Allow	Yes
28	VPN	LAN	Any	WLAN RemoteAccess Networks	Any	Allow	No
29	VPN	LAN	Any	WAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 23

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 # 24

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 25

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 26

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 27

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 28

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 # 29

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

4.1.18 'VPN' to 'WAN'

#	From	To	Source	Destination	Service	Action	Enabled
30	VPN	WAN	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
31	VPN	WAN	Any	All Interface IP	SNMP	Allow	Yes
32	VPN	WAN	Any	All Interface IP	SSH Management	Allow	Yes
33	VPN	WAN	Any	All Interface IP	HTTPS Management	Allow	Yes
34	VPN	WAN	Any	WLAN RemoteAccess Networks	Any	Allow	No
35	VPN	WAN	Any	WAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 30

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 31

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 32

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 33

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 34

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 # 35

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

4.1.19 'VPN' to 'DMZ'

#	From	To	Source	Destination	Service	Action	Enabled
36	VPN	DMZ	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
37	VPN	DMZ	Any	All Interface IP	SNMP	Allow	Yes
38	VPN	DMZ	Any	All Interface IP	SSH Management	Allow	Yes
39	VPN	DMZ	Any	All Interface IP	HTTPS Management	Allow	Yes
40	VPN	DMZ	Any	WLAN RemoteAccess Networks	Any	Allow	No
41	VPN	DMZ	Any	WAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 36

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 37

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 38

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 39

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 40

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 # 41

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

4.1.20 'VPN' to 'VPN'

#	From	To	Source	Destination	Service	Action	Enabled
42	VPN	VPN	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
43	VPN	VPN	Any	All Interface IP	SNMP	Allow	Yes
44	VPN	VPN	Any	All Interface IP	SSH Management	Allow	Yes
45	VPN	VPN	Any	All Interface IP	HTTPS Management	Allow	Yes
46	VPN	VPN	Any	WLAN RemoteAccess Networks	Any	Allow	No
47	VPN	VPN	WLAN RemoteAccess	Any	Any	Allow	No

			Networks				
48	VPN	VPN	Any	WAN RemoteAccess Networks	Any	Allow	No
49	VPN	VPN	WAN RemoteAccess Networks	Any	Any	Allow	No

Details for Access Rule # 42

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 43

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 44

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 45

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 46

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 # 47

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

Details for Access Rule # 48

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 # 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

4.1.21 'VPN' to 'SSLVPN'

#	From	To	Source	Destination	Service	Action	Enabled
50	VPN	SSLVPN	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
51	VPN	SSLVPN	Any	All Interface IP	SNMP	Allow	Yes

52	VPN	SSLVPN	Any	All Interface IP	SSH Management	Allow	Yes
53	VPN	SSLVPN	Any	All Interface IP	HTTPS Management	Allow	Yes
54	VPN	SSLVPN	Any	WLAN RemoteAccess Networks	Any	Allow	No
55	VPN	SSLVPN	Any	WAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 50

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 51

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 52

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 53

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 54

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 # 55

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

4.1.22 'VPN' to 'MULTICAST'

#	From	To	Source	Destination	Service	Action	Enabled
56	VPN	MULTICAST	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
57	VPN	MULTICAST	Any	All Interface IP	SNMP	Allow	Yes
58	VPN	MULTICAST	Any	All Interface IP	SSH Management	Allow	Yes
59	VPN	MULTICAST	Any	All Interface IP	HTTPS Management	Allow	Yes
60	VPN	MULTICAST	Any	WLAN RemoteAccess Networks	Any	Allow	No
61	VPN	MULTICAST	Any	WAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 56

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 57

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 58

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 59

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 60

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 # 61

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

4.1.23 'VPN' to 'WLAN'

#	From	To	Source	Destination	Service	Action	Enabled
62	VPN	WLAN	Any	All Interface IP	SonicpointN Layer3 Management	Allow	Yes
63	VPN	WLAN	Any	All Interface IP	SNMP	Allow	Yes
64	VPN	WLAN	Any	All Interface IP	SSH Management	Allow	Yes
65	VPN	WLAN	Any	All Interface IP	HTTPS Management	Allow	Yes
66	VPN	WLAN	Any	WLAN RemoteAccess Networks	Any	Allow	No
67	VPN	WLAN	Any	WAN RemoteAccess Networks	Any	Allow	No

Details for Access Rule # 62

Source	Any
Destination	All Interface IP
Service	SonicpointN Layer3 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 for VPN enabled management via this SA

Details for Access Rule # 63

Source	Any
Destination	All Interface 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 for VPN enabled management via this SA

Details for Access Rule # 64

Source	Any
Destination	All Interface IP
Service	SSH Management
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 for VPN enabled management via this SA

Details for Access Rule # 65

Source	Any
Destination	All Interface IP
Service	HTTPS Management
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 for VPN enabled management via this SA

Details for Access Rule # 66

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 # 67

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

4.1.24 'SSLVPN' to 'VPN'

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

Details for Access Rule # 68

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

Details for Access Rule # 69

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

4.1.25 'WLAN' to 'LAN'

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

Details for Access Rule # 70

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

4.1.26 'WLAN' to 'WAN'

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

Details for Access Rule # 71

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

4.1.27 'WLAN' to 'DMZ'

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

Details for Access Rule # 72

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 'VPN'

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

Details for Access Rule # 73

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

Details for Access Rule # 74

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

4.1.29 'WLAN' to 'MULTICAST'

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

Details for Access Rule # 75

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

4.1.30 'WLAN' to 'WLAN'

#	From	To	Source	Destination	Service	Action	Enabled
76	WLAN	WLAN	Any	All W0 Management IP	Ping	Allow	Yes
77	WLAN	WLAN	Any	All W0 Management IP	SSH Management	Allow	Yes
78	WLAN	WLAN	Any	All W0 Management IP	HTTPS Management	Allow	Yes
79	WLAN	WLAN	Any	All W0 Management IP	HTTP Management	Allow	Yes

Details for Access Rule # 76

Source	Any
Destination	All W0 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 # 77

Source	Any
Destination	All W0 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 # 78

Source	Any

Destination	All W0 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 # 79

Source	Any
Destination	All W0 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

4.2 App Rules

App Rules Global Settings

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

4.3 App Control Advanced

App Control Global Settings

Enable App Control	off
Enable Logging For All App	off

4.4 Match Objects

no entries

4.5 Action Objects

#	Name	Action Type	Content
1	Block SMTP E-Mail Without Reply	Block SMTP E-Mail Without Reply	
2	Bypass DPI	Bypass DPI	
3	CFS block page	CFS Block Page	
4	No Action	No Action	
5	Packet Monitor	Packet Monitor	
6	Reset/Drop	Reset/Drop	

4.6 Address Objects

4.6.1 Address Groups

#	Name	Type

1	LAN Subnets	Group
2	Firewalled Subnets	Group
3	LAN Interface IP	Group
4	WAN Subnets	Group
5	WAN Interface IP	Group
6	DMZ Subnets	Group
7	DMZ Interface IP	Group
8	WLAN Subnets	Group
9	WLAN Interface IP	Group
10	All WAN IP	Group
11	All Interface IP	Group
12	All X0 Management IP	Group
13	All SonicPoints	Group
14	All Authorized Access Points	Group
15	All Rogue Access Points	Group
16	Default ACL Allow Group	Group
17	Default ACL Deny Group	Group
18	Node License Exclusion List	Group
19	RBL User White List	Group
20	RBL User Black List	Group
21	Public Mail Server Address Group	Group
22	Default Trusted Relay Agent List	Group
23	McAfee Client AV Enforcement List	Group
24	Kaspersky Client AV Enforcement List	Group
25	Excluded from Client AV Enforcement List	Group
26	Client CFS Enforcement List	Group
27	Excluded from Client CFS Enforcement List	Group
28	Default Geo-IP and Botnet Exclusion Group	Group
29	All Rogue Devices	Group
30	SSO Agents	Group
31	Default SonicPoint ACL Allow Group	Group
32	Default SonicPoint ACL Deny Group	Group
33	All X1 Management IP	Group
34	All X2 Management IP	Group
35	All X3 Management IP	Group
36	All X4 Management IP	Group
37	All W0 Management IP	Group
38	All U0 Management IP	Group
39	All U1 Management IP	Group
40	Terminal Services Agents	Group
41	Guest Authentication Servers	Group
42	nacDefault Device Profile for Windows	Group
43	nafDefault Device Profile for Windows	Group

4.6.2 Address Objects

#	Name	Type
1	X0 IP	Host
2	X0 Subnet	Network
3	X1 IP	Host
4	X1 Subnet	Network
5	X2 IP	Host
6	X2 Subnet	Network
7	X3 IP	Host
8	X3 Subnet	Network
9	X4 IP	Host
10	X4 Subnet	Network
11	W0 IP	Host
12	W0 Subnet	Network
13	U0 IP	Host
14	U0 Subnet	Network
15	U1 IP	Host
16	U1 Subnet	Network
17	Default Gateway	Host
18	Secondary Default Gateway	Host
19	Dial-Up Default Gateway	Host
20	Default Active WAN IP	Host
21	X1 Default Gateway	Host
22	WAN RemoteAccess Networks	Network
23	WLAN RemoteAccess Networks	Network

4.7 Service Objects

4.7.1 Service Groups

#	Name	Members
1	AD Directory Services	LDAP, LDAP (UDP), LDAPS, NTP, DNS (Name Service), Kerberos, DCE EndPoint, Host Name Server, AD NetBios Services, RPC Services, RPC Services (IANA)
2	AD Server	DCE EndPoint, AD NetBios Services
3	NT Domain Login	LDAP, Kerberos, NetBios, NT Domain Login Port 1025, DCE EndPoint
4	SonicWALL SSO Agents	
5	SonicWALL TS Agents	
6	Terminal Services	Terminal Services TCP, Terminal Services UDP
7	Citrix	Citrix TCP, Citrix TCP (Session Reliability), Citrix UDP
8	IRC (Chat)	IRC (Chat) 194, IRC (Chat) 6666-6670, IRC (Chat) 7000
9	DNS (Name Service)	DNS (Name Service) TCP, DNS (Name Service) UDP
10	FTP (All)	FTP Data, FTP Control
11	IKE	IKE (Key Exchange), IKE (Traversal)
12	ICMP	Echo Reply, Destination Unreachable, Source Quench, Redirect, Echo, Router Advertisement, Router Solicitation, Time Exceeded
13	Ping	Ping 0, Ping 8
14	Kerberos	Kerberos TCP, Kerberos UDP
15	NetBios	NetBios NS TCP, NetBios NS UDP, NetBios DGM TCP, NetBios DGM UDP, NetBios SSN TCP, NetBios SSN UDP, SMB
16	NFS	NFS TCP, NFS UDP
17	Syslog	Syslog TCP, Syslog UDP
18	VOIP	H323 Call Signaling, H323 Gatekeeper Discovery, H323 Gatekeeper RAS, MGCP TCP, MGCP UDP, SIP, Skinny, T120 (Whiteboard+A43)
19	PC Anywhere	PC Anywhere TCP, PC Anywhere UDP
20	Timbuktu	Timbuktu TCP 407, Timbuktu UDP 407, Timbuktu TCP 1417-1420, Timbuktu UDP 1419
21	Streaming media	RTSP, PNA, MMS
22	RTSP	RTSP TCP, RTSP UDP
23	MMS	MMS TCP, MMS UDP
24	Yahoo Messenger	Yahoo Messenger TCP, Yahoo Messenger UDP
25	VNC	VNC 5500, VNC 5800, VNC 5900
26	P2P Services	Edonkey, WinMX, Kazaa / FastTrack, iMesh, Direct Connect, BearShare
27	Edonkey	Edonkey TCP, Edonkey UDP
28	WinMX	WinMX TCP 6699, WinMX TCP 7729-7735, WinMX UDP 6257
29	IGMP	Membership Query, V2 Membership Report, Leave Group, V3 Membership Report
30	Multicast RTP	
31	ShoreTel	ShoreTel Call Control, ShoreTel RTP, ShoreTel IP Phone Control 2427, ShoreTel IP Phone Control 2727
32	Tivo Services	Tivo TCP Beacon, Tivo UDP Beacon, Tivo TCP Data, Tivo TCP Desktop (8101/8102), Tivo TCP Desktop (8200)
33	Host Name Server	Host Name Server TCP, Host Name Server UDP
34	AD NetBios Services	SMB, NetBios TCP, NetBios UDP
35	ICMPv6	Destination Unreachable (IPv6), Packet Too Big, Time Exceeded (IPv6), Parameter Problem, Echo (IPv6), Echo Reply (IPv6)
36	Neighbor Discovery	Router Solicitation (IPv6), Router Advertisement (IPv6), Neighbor Solicitation, Neighbor Advertisement, Redirect (IPv6)
37	Ping6	Ping6 128, Ping6 129
38	OSPF	Hello, Dbd, Lsr, Lsu, Lsa

4.7.2 Service Objects

#	Name	Protocol	Port Start	Port End
1	HTTP	TCP	80	80
2	HTTP Management	TCP	80	80
3	HTTPS	TCP	443	443
4	HTTPS Management	TCP	443	443
5	RADIUS Accounting	UDP	1813	1813
6	IDENT	TCP	113	113
7	IMAP3	TCP	220	220
8	IMAP4	TCP	143	143
9	ISAKMP	UDP	500	500
10	LDAP	TCP	389	389
11	LDAP (UDP)	UDP	389	389
12	LDAPS	TCP	636	636
13	LPR (Unix Printer)	TCP	515	515
14	MS SQL	TCP	1433	1433

15	NNTP (News)	TCP	119	119
16	NTP	UDP	123	123
17	POP3 (Retrieve E-Mail)	TCP	110	110
18	Terminal Services TCP	TCP	3389	3389
19	Terminal Services UDP	UDP	3389	3389
20	PPTP	TCP	1723	1723
21	SMTP (Send E-Mail)	TCP	25	25
22	SNMP	UDP	161	162
23	SQL*Net	TCP	1521	1521
24	SSH	TCP	22	22
25	Telnet	TCP	23	23
26	TFTP	UDP	69	69
27	Citrix TCP	TCP	1494	1494
28	Citrix TCP (Session Reliability)	TCP	2598	2598
29	Citrix UDP	UDP	1604	1604
30	IRC (Chat) 194	TCP	194	194
31	IRC (Chat) 6666-6670	TCP	6666	6670
32	IRC (Chat) 7000	TCP	7000	7000
33	DNS (Name Service) TCP	TCP	53	53
34	DNS (Name Service) UDP	UDP	53	53
35	Enhanced TV	TCP	9000	9000
36	ESP (IPSec)	IPSEC_ESP	1	1
37	FTP	TCP	21	21
38	FTP Data	TCP	20	20
39	FTP Control	TCP	21	21
40	Gopher	TCP	70	70
41	IKE (Key Exchange)	UDP	500	500
42	IKE (Traversal)	UDP	4500	4500
43	Lotus Notes	TCP	1352	1352
44	Echo Reply	ICMP	0	0
45	Destination Unreachable	ICMP	3	3
46	Source Quench	ICMP	4	4
47	Redirect	ICMP	5	5
48	Echo	ICMP	8	8
49	Router Advertisement	ICMP	9	9
50	Router Solicitation	ICMP	10	10
51	Time Exceeded	ICMP	11	11
52	Ping 0	ICMP	0	0
53	Ping 8	ICMP	8	8
54	Kerberos TCP	TCP	88	88
55	Kerberos UDP	UDP	88	88
56	NetBios NS TCP	TCP	137	137
57	NetBios NS UDP	UDP	137	137
58	NetBios DGM TCP	TCP	138	138
59	NetBios DGM UDP	UDP	138	138
60	NetBios SSN TCP	TCP	139	139
61	NetBios SSN UDP	UDP	139	139
62	SMB	TCP	445	445
63	NFS TCP	TCP	2049	2049
64	NFS UDP	UDP	2049	2049
65	Syslog TCP	TCP	514	514
66	Syslog UDP	UDP	514	514
67	H323 Call Signaling	TCP	1720	1720
68	H323 Gatekeeper Discovery	UDP	1718	1718
69	H323 Gatekeeper RAS	UDP	1719	1719
70	MGCP TCP	TCP	2428	2428
71	MGCP UDP	UDP	2427	2427
72	SIP	UDP	5060	5061
73	Skinny	TCP	2000	2000
74	T120 (Whiteboard+A43)	TCP	1503	1503
75	PC Anywhere TCP	TCP	5631	5631
76	PC Anywhere UDP	UDP	5632	5632
77	Timbuktu TCP 407	TCP	407	407
78	Timbuktu UDP 407	UDP	407	407
79	Timbuktu TCP 1417-1420	TCP	1417	1420
80	Timbuktu UDP 1419	UDP	1419	1419
81	RTSP TCP	TCP	554	554
82	RTSP UDP	UDP	554	554
83	PNA	TCP	7070	7070
84	MMS TCP	TCP	1755	1755
85	MMS UDP	UDP	1755	1755
86	Squid	TCP	3128	3128
87	Yahoo Messenger TCP	TCP	5050	5050
88	Yahoo Messenger UDP	UDP	5050	5050
89	VNC 5500	TCP	5500	5500
90	VNC 5800	TCP	5800	5800

91	VNC 5900	TCP	5900	5900
92	Remotely Anywhere	TCP	2000	2000
93	Remotely Possible	TCP	799	799
94	Quake	UDP	27910	27910
95	cu-seeme	UDP	24032	24032
96	Edonkey TCP	TCP	4661	4662
97	Edonkey UDP	UDP	4665	4665
98	WinMX TCP 6699	TCP	6699	6699
99	WinMX TCP 7729-7735	TCP	7729	7735
100	WinMX UDP 6257	UDP	6257	6257
101	Kazaa / FastTrack	TCP	1214	1214
102	iMesh	TCP	4000	5000
103	Direct Connect	TCP	411	412
104	BearShare	TCP	6346	6349
105	ZebTelnet	TCP	2601	2620
106	Membership Query	IGMP	17	17
107	V2 Membership Report	IGMP	22	22
108	Leave Group	IGMP	23	23
109	V3 Membership Report	IGMP	34	34
110	GMS HTTPS	TCP	3003	3003
111	Radius	UDP	1812	1812
112	GSCTrace	TCP	59162	59162
113	SSH Management	TCP	22	22
114	NT Domain Login Port 1025	TCP	1025	1025
115	DCE EndPoint	TCP	135	135
116	External Guest Authentication	TCP	4043	4043
117	ShoreTel Call Control	UDP	5440	5446
118	ShoreTel RTP	UDP	5004	5004
119	ShoreTel IP Phone Control 2427	UDP	2427	2427
120	ShoreTel IP Phone Control 2727	UDP	2727	2727
121	Tivo TCP Beacon	TCP	2190	2190
122	Tivo UDP Beacon	UDP	2190	2190
123	Tivo TCP Data	TCP	8080	8089
124	Tivo TCP Desktop (8101/8102)	TCP	8101	8102
125	Tivo TCP Desktop (8200)	TCP	8200	8200
126	IPcomp	IPComp	1	1
127	Apple Bonjour	UDP	5353	5353
128	SMTP (Anti-Spam Inbound Port)	TCP	25	25
129	SSLVPN	TCP	4433	4433
130	SonicpointN Layer3 Management	GRE	41321	41321
131	6over4	IPv6	1	1
132	Host Name Server TCP	TCP	42	42
133	Host Name Server UDP	UDP	42	42
134	NetBios TCP	TCP	137	139
135	NetBios UDP	UDP	137	139
136	RPC Services	TCP	1025	5000
137	RPC Services (IANA)	TCP	49152	65535
138	DRP	TCP	59160	59160
139	NetFlow / IPFIX	UDP	2055	2055
140	BGP	TCP	179	179
141	Destination Unreachable (IPv6)		1	1
142	Packet Too Big		2	2
143	Time Exceeded (IPv6)		3	3
144	Parameter Problem		4	4
145	Echo (IPv6)		128	128
146	Echo Reply (IPv6)		129	129
147	Router Solicitation (IPv6)		133	133
148	Router Advertisement (IPv6)		134	134
149	Neighbor Solicitation		135	135
150	Neighbor Advertisement		136	136
151	Redirect (IPv6)		137	137
152	Ping6 128		128	128
153	Ping6 129		129	129
154	GRE	GRE	1	1
155	Hello		1	1
156	Dbd		2	2
157	Lsr		3	3
158	Lsu		4	4
159	Lsa		5	5

4.8 Bandwidth Objects

#	Name	Guaranteed	Maximum	Priority	Violation Action

1	Default Action Object BWM Egress High	0 Mbps	10 Mbps	0 Realtime	Delay
2	Default Action Object BWM Ingress High	0 Mbps	10 Mbps	0 Realtime	Delay
3	Default Action Object BWM Egress Medium	0 Mbps	5 Mbps	5 Medium Low	Delay
4	Default Action Object BWM Ingress Medium	0 Mbps	5 Mbps	5 Medium Low	Delay
5	Default Action Object BWM Egress Low	0 Mbps	1 Mbps	7 Lowest	Delay
6	Default Action Object BWM Ingress Low	0 Mbps	1 Mbps	7 Lowest	Delay

4.9 Email Addr Objects

no entries

5. Firewall Settings

5.1 Advanced

Detection Prevention

Enable Stealth Mode	off
Randomize IP ID	off
Decrement IP TTL for forwarding traffic	off
Never generate ICMP Time-Exceeded packets	off

Dynamic Ports

Enable FTP Transformations for TCP port(s) in Service Object	FTP (All)
Enable support for Oracle (SQLNet)	on
Enable RTSP Transformations	on

Source Routed Packets

Drop source routed IP packets	on

Connections

DPI Connections (DPI services enabled with additional performance optimizations)

Access Rule Options

Force inbound/outbound FTP to use port 20	off
Apply firewall rules for intra-LAN traffic to/from the same interface	
Always issue RST for discarded outgoing TCP connections	

IP and UDP Checksum Enforcement

Enable IP header checksum enforcement	off
Enable UDP checksum enforcement	off
Default UDP connection timeout (seconds)	30

5.2 BWM

Bandwidth Management Type: None

Priority	Enable	Guaranteed	MaximumBurst
0 Realtime	0	0.000	100.000
1 Highest	0	0.000	100.000
2 High	1	30.000	100.000
3 Medium High	0	0.000	100.000
4 Medium	1	50.000	100.000
5 Medium Low	0	0.000	100.000
6 Low	1	20.000	100.000
6 Lowest	0	0.000	100.000

5.3 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	off
UDP Flood Attack Threshold (UDP Packets / Sec)	1000
UDP Flood Attack Blocking Time (Sec)	2
UDP Flood Attack Protected Destination List	

ICMP Flood Protection

Enable ICMP Flood Protection	off
ICMP Flood Attack Threshold (ICMP Packets / Sec)	200
ICMP Flood Attack Blocking Time (Sec)	2
ICMP Flood Attack Protected Destination List	

5.4 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

5.5 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

5.6 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)	3600
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	
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	0017C5B5870C

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	off
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	off
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	LocalDomain
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. Users

11.1 Settings

User Login Settings

Authentication method for login	Local Users
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	WAN Zone	Public Zones	Wireless Zones	VPN Zone
	on	off	on	off	off
Window size (pixels)	460 x 310				
Enable scroll bars on the window					

Acceptable use policy page content

11.2 Local Groups

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

11.3 Guest Services

Global Guest Settings

Show guest login status window with logout button	on

Guest Profiles	Bypass Filters	Guest Services	Admin	Comment
Default				

12. High Availability

12.1 Settings

High Availability Settings

Enable High Availability	off

SonicWALL Address Settings

Primary SonicWALL Serial Number	0017C5B5870C
Backup SonicWALL Serial Number	000000000000

12.2 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)	1000
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

12.3 High Availability Monitoring Settings

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

13. Security Services

13.1 Summary

Security Services Settings

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

13.2 Content Filter

Content Filter Type

SonicWALL CFS

SonicWALL CFS Settings

Enable IP based HTTPS Content Filtering	off
Enable CFS Server Failover	off
Enable CFS Wire Mode	off
If Server is unavailable for (secs)	5
	Allow traffic to all Web sites
If URL marked as Forbidden	
Block Access to URL	on
Log Access to URL	on

URL Cache

Cache Size (KB)	1536

Policies

Custom List

Allowed Domains
Forbidden Domains
Keyword Blocking

Options

Enable Allowed/Forbidden Domains	on
Enable Keyword Blocking	on
Disable all web traffic except for Allowed Domains	off

Web Usage Consent

Require Consent	off
Maximum Web Usage (minutes)	0
User Idle Timeout (minutes)	15
Consent Page URL (optional filtering)	
Consent Accepted URL (filtering off)	
Consent Accepted URL (filtering on)	

Mandatory IP Filtering

Consent Page URL (mandatory filtering)	
Filtered IP Address	

Restrict Web Features

ActiveX	off
Java	off
Cookies	off
Access to HTTP Proxy Servers	off

Message to Display when Blocking

13.3 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

13.4 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

HTTP Clientless Notification

Enable HTTP Clientless Notification Alerts	on

Message to Display when Blocking

This request is blocked by the Firewall 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			
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	

13.5 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

13.6 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

13.7 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

13.8 GeoIP Filter

General

Block connections to/from selected countries	All
Enable Logging	off

Geo-IP Exclusion Object

Default Geo-IP and Botnet Exclusion Group

13.9 Botnet Filter

General

Block connections to/from Botnet Command and Control Servers	All
Enable Logging	off

Botnet Exclusion Object

Default Geo-IP and Botnet Exclusion Group

14. AppFlow

14.1 Flow Reporting

Settings

Send AppFlow To Local Collector	off
Enable Real-Time Data Collection	off
Collect Real-Time Data For	Top apps, Bits per sec., Packets per sec., Average packet size, Connections per sec., Core util.
Enable Aggregate AppFlow Report Data Collection	off

AppFlow Server Settings

Send AppFlow To SonicWALL AppFlow Server	off
Send Real-Time Data To SonicWALL AppFlow Server	off

External Collector Settings

Send AppFlow and Real-Time Data To External Collector	off
External AppFlow Reporting Format	Netflow version-5
External Collector's IP address	0.0.0.0
Source IP To Use For Collector On A VPN tunnel	0.0.0.0
External Collector's UDP Port Number	2055
Send IPFIX/Netflow Templates At Regular Interval	on
Send Static AppFlow At Regular Interval	on
Send Static AppFlow For Following Tables	Applications, Viruses, Spyware, Intrusion, Services, Rating Map
Send Dynamic AppFlow For Following Tables	Connections, Users, URLs, URL ratings, VPNs, VOIPs
Include Following Additional Reports via IPFIX	

Connection Report Settings

Report Connections	All
Report On Connection OPEN	on
Report On Connection CLOSE	on
Report Connection On Active Timeout	off
Number Of Seconds	60
Report Connection On Kilo BYTES Exchanged	off
Kilobytes Exchanged	100
Report ONCE	on
Report Connections On Following Updates	threat detection, application detection, user detection, VPN tunnel detection

Other Report Settings

Report DROPPED Connection	on
Skip Reporting STACK Connections	on
Include Following URL Types	Gifs, Jpegs, Pngs, Htmls, Aspx
Enable Geo-IP And Domain Resolution	

14.2 AppFlow Server

Configured AppFlow Server

Enable Keep-Alive with AppFlow Server	on
AppFlow Server Address	0.0.0.0
Source IP to use over VPN Tunnel	0.0.0.0
AppFlow Server Max Flows	200000
Server Communication Timeout	60
Firewall Name	My SonicWALL
Connection Passphrase	XXXXXXXX
Auto-Synchronize AppFlow Server	off

15. Log

15.1 Categories

Log Severity/Priority

Logging Level	Debug	Log Redundancy Filter (seconds)	

Category	Description	Log	Alerts	Syslog
802.11b Management	Legacy category			
Advanced Routing	ARS Logging			
Application Firewall	Application Firewall Activity			
Attacks	Legacy category			
Authenticated Access	Adminstrator, user, and guest account activity			

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

15.2 Syslog

Syslog Settings

Syslog Facility	Local Use 0
Override Syslog Settings with ViewPoint Settings	off
Syslog Event Redundancy Filter (seconds)	0
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
Created by autoDOC