Managed Firewall
Service Description and Service Level Agreements

Your relationship with Dell

This Service Description and Service Level Agreement is provided for the customer ("You" or "Customer") and the Dell entity identified in Customer's Service Order for the purchase of this Service (defined below). This Service is provided in connection with Customer's separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security services. In the absence of either a master services agreement or security services schedule, this service is provided in connection with the Dell SecureWorks Master Services Agreement, available at http://Dell.com/SecurityTerms and incorporated by reference in its entirety herein.

1 SERVICE OVERVIEW

The Dell Managed Firewall Service (the "Service") provides 24x7x365 proactive administration of your SonicWALL infrastructure. The Service is comprised of support for the following components.

Intrusion Prevention Service
Firewall
Anti-Virus Protection
Application Intelligence and Control
Anti-Spyware
Content & URL Filtering (CFS)
Wireless LAN support
VPN Tunnels *
Multi-WAN Support

* Appropriate to services selected.

2 SERVICE DESCRIPTION

Dell's proprietary platform provides the foundation for delivery of our managed security services (the "Dell Portal"). This Dell-developed technology facilitates device management, health monitoring, security analysis and customer reporting. The following service components are included with Service:

- Device availability monitoring
- Security Event Monitoring
- Upgrade and Patch Management
- Change Management
- VPN Configuration

2.1 Device Availability Monitoring

Dell must be able to connect to the device via the Internet using HTTPS & IPSEC protocol.

Dell will perform availability monitoring of the device. Dell monitors availability via periodic polling of the device. If periodic polling checks indicate that the device has become unavailable, an automatic alert is sent to Dell which then generates a ticket for the customer to view on the Dell Portal.

If the root problem of device failure is customer related, such as a network change, outage, or customer-managed device, Dell will provide customer with troubleshooting information upon customer request but Dell is not responsible for troubleshooting issues that are not directly related to the device under management.

2.2 Security Event Monitoring

SonicWALL log data is gathered by the Global Management System located at Dell's premise. The data is parsed, correlated, and prioritized. The relevant security events are categorized by Dell based on the severity level. Malicious and unknown events are correlated and alerts are presented to Customer via the Dell Portal.

The Dell Portal provides customers with a secure, web-based method to monitor the enterprise, generate security reports and update escalation procedures.

Following deliverables are associated with Security Event Monitoring Service

- Dell Portal access for ticket requests and reporting capabilities.
- Ongoing enterprise security event aggregation and reporting for devices during the service term.

Incident response, forensics and ticket requests associated with security event analysis are not included in security event monitoring service.

2.3 Software Upgrade and Patch Maintenance

As security related software patches and upgrades are released by SonicWALL, Dell assesses the applicability of each release to Customer's environment. Dell will work with Customer to schedule any necessary remote upgrades if necessary.

Customer owned equipment upgrades are implemented by Dell as part of the selected service, so long as the following conditions apply:

- The upgrade can be performed remotely, either independently or with a minimal amount of on-site assistance by Customer.
- The upgrade does not require a change to underlying hardware on which the Customer owned equipment is deployed.

In cases where support for a particular product or product version is being discontinued by the vendor or by Dell, Dell will communicate new platform migration options. In order to be assured of uninterrupted service, Customer must complete the migration process within sixty (60) days. Customer bears any costs relating to procuring new hardware or components and to re-provisioning any devices.

SLAs do not apply during maintenance work. SLAs cannot be guaranteed if Customer does not make the changes required by Dell or if Customer otherwise prevents Dell from making the changes it notifies Customer are necessary for continued Service.

2.4 Change Management

Customer may submit change requests to Dell via the Customer portal. Dell requires that the change request is made by an authorized Customer contact. Dell will contact Customer via email or customer portal to clarify unclear requests as needed. The Change Management request could be on any of the following features of the SonicWALL appliance.

2.4.1 Firewall

Dell will manage the policy on the device.

The following defines what is considered to be one policy change:

- Adding, deleting, or modifying up to three individual Network Address Translations (NAT) (incoming, outgoing and loop-back) including object creation
- Adding, deleting, or modifying up to two access control list changes (such as permit or deny changes) Including the creation of up to 6 policy objects creation (Hosts, Groups, Networks, Ranges and Service objects)
- Adding, deleting, or modifying up to two individual network routes within the firewall

Standard policy change may comprise one or more of the above bullets. Any change request that is not specifically listed above may be completed by Dell on a time and materials basis. Dell reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of Customer's service.

Dell does not design or validate rule sets or provide troubleshooting related to rule sets as part of the Service.

2.4.2 Intrusion Prevention System

Dell manages the policy on the device. Policies are updated regularly as updates are released by vendors and reviewed by Dell.

The following defines what is considered to be one policy change:

- Adding, deleting, or modifying IDS/IPS signatures, not including routine signature updates

Any change request that is not specifically listed above may be completed by Dell on a time and materials basis. Dell reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of Customer's service.

2.4.3 Application Intelligence and Control

Dell can enable application control as per Customer's request. There are over 1600 applications supported within the SonicWALL firewall, therefore it is Customer's responsibility to specify all application control and application rule settings required. Dell will configure the SonicWALL firewall in accordance with the Customer's specifications.

Dell does not offer application debugging in the event of unexpected consequences from application control settings. Dell's responsibilities surrounding application control are limited to enabling or disabling the application control settings. At the time of initial deployment, by default, application intelligence and control is turned off.

2.4.4 Anti-Virus Protection support

Dell can enable Gateway anti-virus ("GAV" hereafter) functionality on managed SonicWALL devices. As a component of this service, Dell will work with SonicWALL to update GAV policies regularly as updates are released by SonicWALL and reviewed by Dell.

Security relevant AV events are logged to the customer portal. These events will not result in ticket creation or viewing by a Dell SOC Analyst.

Enforced Client AV protection is not supported.

2.4.5 Anti-Spyware

Dell can enable Gateway anti-spyware ("GAS" hereafter) functionality on managed SonicWALL devices. As a component of this service, Dell will update GAS policies regularly as updates are released by SonicWALL and reviewed by Dell.

Security relevant GAS events are logged to the customer portal. These events will not result in ticket creation or viewing by a Dell SOC Analyst.

2.4.6 Content & URL Filtering (CFS) support

Where CFS as a licensed option is purchased, Dell shall deploy the default categorization policy by zone or internet protocol ("IP") range as specified by the Customer. Web sites that are accessed that are within an enabled category shall be blocked. Customers who wish to challenge a categorization shall contact SonicWALL directly.

Customers can request, via the Dell Portal, change of category. This is equated to a standard policy change request. Requests for whitelisting or blacklisting of domains are permitted under a standard policy change request. User authentication for CFS service is not supported.

2.4.7 Wireless LAN support

Dell will deploy a trusted network, a guest network (2 SSID's), and up to 8 SonicPoints.
The following defines what is considered to be one policy change:

- Addition/deletion of a SonicPoint
- Modification of an SSID
- Modification of a pre-shared key

It is customer's responsibility to configure the LAN infrastructure connecting to SonicPoints. Dell will not perform wireless LAN availability monitoring and cannot assist with individual wireless client connectivity issues

2.4.8 Multi-WAN Support

At set-up time, the Customer can specify single WAN (Ethernet) or multi-WAN (Ethernet and 3G). It is the Customer's responsibility to provide and maintain the 3G service. Dell shall set-up and test multi-WAN functionality.

The following defines what is considered to be one policy change:

- Change of ISP connection or network preference.

Dell is not responsible for advising Customers about network priority changes.

2.5 VPN Configuration

Dell configures VPN connections for firewalls contractually managed by Dell and troubleshoots the firewall in the event of an outage. At least one (1) firewall must be managed by Dell to provide this Service. Details on number of VPN tunnel configurations based on an appliance model is given below. Site-to-site VPN configuration is based on Dell standard VPN templates. No warranty is provided on the ability of the managed SonicWALL to successfully interwork with 3rd party firewalls managed by other parties. Dell is unable to provide assistance on remote device configuration.

Dell can configure the managed SonicWALL device to accept connections from Global VPN Client ("GVC"). It is the Customer's responsibility to configure GVC.

Max Users	# of Site to Site VPN Tunnels configurations
TZ 100 series	2
TZ 200 series	5
TZ 215 series	5
NSA 2xxx series	10

2.6 Other Services

Any other services are out-of-scope. Examples of such out-of-scope support include but are not limited to:

- On-site installation and provisioning of device.
- Integration of complementary products that are not managed by Dell (e.g., encrypted email; web reporting software).
- Custom analysis and/or custom reports.
- Forensics.
- Any change requests not specified above.
- Configuration of any tunnel end point that is not terminated on a Dell -managed device.
- Rule set design, validation, and troubleshooting.
- Firewall policy auditing, policy/rule utilization, and security best practice consulting
- Development of customized signatures.

3 SERVICE IMPLEMENTATION

Terms associated with service implementation are described below.

- New SonicWALL devices shall be shipped from Dell directly to the Customer. Shipping costs shall be borne by the Customer.
- New SonicWALL devices shall be deployed and configured remotely by Dell with a standard deployment configuration and on-site support from the customer.
- Existing equipment in use is provisioned remotely, with on-site support from Customer.
- SonicWALL remote start-up and configuration includes the following configuration deliverables. Based on appliance model, firmware version or customer requirements, not all deliverables may be applicable. Any configuration requests not included as a part of standard configuration deliverable must be directed to Dell SecureWorks as a standard change request.
    - Loading the latest firewall firmware
    - Activating the service license keys and enabling security services
    - Configuring administrator accounts
    - Specifying mode of operation, zones, IP address, subnet mask, hostname, static routes, DNS, SYSLOG
    - Setting up the firewall policy consisting of the following elements. Firewall access rules, Network address translation rules, VLAN creation and Object creation (Hosts, Groups, Networks, Ranges and Service objects) as described in table below
    - Enabling wireless security features (wireless appliances only) – intrusion detection and wireless guest services. Service does not include wireless configuration on end Customer devices (eg. Laptops or Mobile devices)
    - Setting up VPNs: site-to-site and Customer-to-site (depends on appliance model as defined in section 2.5)
    - Setting up SSL VPN for remote access (on-firewall local user authentication database is not supported).Setting up user level authentication using external authentication servers where the customer has provided all the required authentication server parameters.
    - Setting up single WAN interface only

Max Users	Maximum # of policy elements
TZ 100 series	30
TZ 200 series	40
TZ 215 series	50
NSA 2xxx series	75

- Dell provides telephone support to Customer contact at the implementation site during installation of all Customer premises equipment.

- Once Customer premise equipment is in place, Dell accesses the device(s) remotely and performs the remaining configuration and service activation tasks which may require device downtime.

Customers must provide Dell with exclusive administrative privileges on the specific devices to be managed. Firewall policy migration services are not included as a part of the managed SonicWALL Service.

Dell will provide Customer with a notice of service commencement, which identifies the service commencement date, when the following conditions have been met: Dell has: (a) established communication with the relevant Customer device(s) (b) verified availability of customer data on the portal; and (c) established communications via SonicWALL Global Management System.

4 CUSTOMER REQUIREMENTS

Customer agrees to perform the following obligations and acknowledges and agrees that Dell's ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

4.1 Hardware/Software Procurement

The Customer is responsible for purchasing the firewall hardware and software necessary for Dell to deliver the Service. Additionally, the Customer is responsible for ensuring that their hardware/software stays within SonicWALL's supported versions. Dell's SLAs will not apply to platforms that are end of life, end of support, or are otherwise not receiving updates by the vendor.

4.2 Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance for the Customer-owned firewall and connectivity to prevent network performance degradation and maintain communications between the customer's contracted firewall devices and Dell's security operations centers (Secure Operations Centers" or "SOC(s)"). Customer is required to purchase SonicWALL Comprehensive Gateway Security Suite ("CGSS") to enable SecureWorks to deliver the Service. Dell's SLA's will not apply to managed SonicWALL devices not subscribed to SonicWALL CGSS.

4.3 RMA Responsibilities

The Customer is responsible for initiating and fulfilling the return materials authorization ("RMA") process directly with SonicWALL in the event that the hardware/software being managed by Dell is determined to be in a failed or faulty state and requires replacement.

4.4 Connectivity

Customer will provide access to Customer-premises and relevant appliance(s) necessary for Dell to manage and monitor the contracted firewall devices. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Dell customer portal. Service activation which may require device downtime will depend on customer

deliverables such as on-site assistance with initial configuration of the appliance to get connectivity between SonicWALL appliance and Dell data centers. SLAs will not apply to devices that are experiencing Customer-caused connectivity issues.

4.5 Export

Customer acknowledges that the Products, Software and Services provided under this agreement, which may include technology and encryption, are subject to the customs and export control laws and regulations of the United States, and may be rendered or performed either in the U.S., in countries outside the U.S., or outside of the borders of the country in which you or your system is located, and may also be subject to the customs and export laws and regulations of the country in which the Products, Software or Services are rendered or received. Customer agrees to abide by those laws and regulations.

5 SERVICE LEVELS

Service Level Matrix

Service	Standard SLA	SLA Credit
Standard Change Requests	Acknowledgement of receiving the change within two business days from the time stamp on the ticket created by Dell. 1 Per day per device up to max. 5 per month across all service modules (FW, IPS, GAV, Anti-spyware, CFS, WLAN & Multi-WAN).	1/30th of monthly fee for Service for the affected device
Security Event Monitoring	Customer shall receive an alert either through the ticketing system or email within thirty (30) minutes of the determination by Dell that given malicious activity constitutes a possible security incident.	1/30th of monthly fee for Service for the affected device
Active Health Monitoring	Device Unreachable – Customer shall receive a notification either through the ticketing system or email within 1 hour from identification of the device being unreachable.	1/30th of monthly fee for Service for the affected device

6 ADDITIONAL SERVICE RULES, REGULATIONS AND CONDITIONS

a. The Service provides robust device management, security event analysis and performance monitoring to the Customer. Deployment of the Service does not achieve the impossible goal of risk elimination, and therefore Dell does not guarantee that intrusions, compromises, or other unauthorized activity will not occur on Customer's network.

b. Dell may schedule maintenance outages for Dell-owned equipment/servers which are being utilized to perform the services with 24 hours' notice to designated Customer contacts.

c. The Service Levels set forth herein are subject to the following terms, conditions and limitations:

i. The Service Levels shall not apply during scheduled maintenance outages and therefore are not eligible for any Service Level credit. Dell shall not be held liable for any Service impact or Service Levels Agreements related to product configurations that are not supported by Dell within the Customer's policy.

ii. The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Dell from providing the Service, delivering the Service Levels or managed service descriptions, including but not limited to: Customer misconduct, Customer negligence, inaccurate or incomplete information provided by the Customer, Customer modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by the Customer, its employees, agents, or third parties acting on behalf of Customer.

iii. The Service Levels shall not apply to the extent Customer does not fulfill and comply with the Customer obligations set forth in this SLA. The obligation of Dell to meet the Service Levels with respect to any incident response or ticket request are conditioned upon Dell's ability to connect directly to the Customer devices on the Customer network through an authenticated server in the Dell Secure Operations Center.

d. Customer will receive credit for any failure to meet the Service Levels outlined above within thirty (30) days of notification by Customer to Dell of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Dell within thirty (30) days of such failure. Dell will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.