CITY OF GRAND JUNCTION/MESA COUNTY, COLORADO

****

CONTRACT

This CONTRACT made and entered into this **17th** day of **December, 2015** by and between the **City of Grand Junction, Colorado,** a government entity in the County of Mesa, State of Colorado, hereinafter in the Contract Documents referred to as the "Owner" and **Sanity Solutions Inc.,** hereinafter in the Contract Documents referred to as the "Contractor."

WITNESSETH:

WHEREAS, the Owner advertised that sealed Responses would be received for furnishing all labor, tools, supplies, equipment, materials, and everything necessary and required for the Project described by the Contract Documents and known as **Replacement Firewall RFP-4089-15-NJ.**

WHEREAS, the Contract has been awarded to the above named Contractor by the Owner, and said Contractor is now ready, willing and able to perform the Work specified in the Notice of Award, in accordance with the Contract Documents;

NOW, THEREFORE, in consideration of the compensation to be paid the Contractor, the mutual covenants hereinafter set forth and subject to the terms hereinafter stated, it is mutually covenanted and agreed as follows:

ARTICLE 1

Contract Documents: It is agreed by the parties hereto that the following list of instruments, drawings, and documents which are attached hereto, bound herewith, or incorporated herein by reference constitute and shall be referred to either as the "Contract Documents" or the "Contract", and all of said instruments, drawings, and documents taken together as a whole constitute the Contract between the parties hereto, and they are fully a part of this agreement as if they were set out verbatim and in full herein:

The order of contract document governance shall be as follows:

a. The body of this contract agreement
b. Solicitation Documents for the Project; **RFP-4089-15-NJ;**
c. Sanity Solutions Quote #006255 – Attachment A
d. Intent to Award
e. Contractors Response to the Solicitation

ARTICLE 2

Definitions: The clauses provided in the Solicitation apply to the terms used in the Contract and all the Contract Documents.

ARTICLE 3

Contract Work: The Contractor agrees to furnish all labor, tools, supplies, equipment, materials, and all that is necessary and required to complete the tasks associated with the Work described, set forth, shown, and included in the Contract Documents as indicated in the Solicitation Document.

ARTICLE 4

Contract Price and Payment Procedures: The Contractor shall accept as full and complete compensation for the performance and completion of all of the Work specified in the Contract Documents, the sum of **Seventy Three Thousand Seven Hundred Sixty Five and 00/100 dollars. ($73,765.00).** If this Contract contains unit price pay items, the Contract Price shall be adjusted in accordance with the actual quantities of items completed and accepted by the Owner at the unit prices quoted in the Solicitation Response. The amount of the Contract Price is and has heretofore been appropriated by the Grand Junction City Council or Mesa County Board of County Commissioners for the use and benefit of this Project. The Contract Price shall not be modified except by Change Order or other written directive of the Owner. The Owner shall not issue a Change Order or other written directive which requires additional work to be performed, which work causes the aggregate amount payable under this Contract to exceed the amount appropriated for this Project, unless and until the Owner provides Contractor written assurance that lawful appropriations to cover the costs of the additional work have been made.

ARTICLE 5

Contract Binding: The Owner and the Contractor each binds itself, its partners, successors, assigns and legal representatives to the other party hereto in respect to all covenants, agreements and obligations contained in the Contract Documents. The Contract Documents constitute the entire agreement between the Owner and Contractor and may only be altered, amended or repealed by a duly executed written instrument. Neither the Owner nor the Contractor shall, without the prior written consent of the other, assign or sublet in whole or in part its interest under any of the Contract Documents and specifically, the Contractor shall not assign any moneys due or to become due without the prior written consent of the Owner.

ARTICLE 6

Severability: If any part, portion or provision of the Contract shall be found or declared null, void or unenforceable for any reason whatsoever by any court of competent jurisdiction or any governmental agency having the authority thereover, only such part, portion or provision

shall be effected thereby and all other parts, portions and provisions of the Contract shall remain in full force and effect.

IN WITNESS WHEREOF, City of Grand Junction/Mesa County, Colorado, has caused this Contract to be subscribed and sealed and attested in its behalf; and the Contractor has signed this Contract the day and the year first mentioned herein.

The Contract is executed in two counterparts.

CITY OF GRAND JUNCTION

DocuSigned by:
By: Jim Finlayson 9575D1DCFD794F2... 12/17/2015 | 08:38 MT
Title: Jim Finlayson, Information Technology Director Date

(SANITY SOLUTIONS INC.)

DocuSigned by:
By: Keith Barnholt 0224D0543B0A4EC... 12/17/2015 | 10:02 MT
Title: Keith Barnholt Keith Barnholt, Account Executive Date

Attachment A - RFP-4089-15-NJ

Phone: Email: kbarnholt@sanitysolutions.com Web: www.sanitysolutions.com

SuperMassive 9400 Solution

Quote # 006255

Version 1

Prepared for

City of Grand Junction

SuperMassive 9400 Solution

Quote Information:

Quote #: 006255
Version: 1
Delivered: 12/07/2015
Expires: 01/06/2016

Prepared for:

City of Grand Junction
Richard White
250 North 5th Street
Grand Junction, CO 81501-2668
richardw@ci.grandjct.co.us
(970) 244-1526

Prepared by:

Sanity Solutions Inc.
Keith Barnholt
720-289-3029
kbarnholt@sanitysolutions.com

Hardware		Price	Qty	Ext. Price
uufw-A6833422	**Dell SonicWALL SuperMassive 9400 Next Generation Firewall** Includes Comprehensive Gateway Security Suite 2 Years 24x7 Gold Support & Maintenance Includes: 6x 10GB SFP+ COPPER W 3M TWINAX CABLE 3X 10GB SFP+ COPPER W 1M TWINAX CABLE	$57,448.00	1	$57,448.00
UUFW-A6833467	**Dell SonicWALL SuperMassive 9400 High Availability Appliance** 2nd Unit- Both Appliances Configured Equally	$24,497.00	1	$24,497.00
uufw-A7487614	**Dell SonicWALL SSL VPN- 25 Users**	$350.00	1	$350.00
uufw-a7483569	**Dell SonicWALL Analyzer**	$950.00	1	$950.00
		Hardware Subtotal		**$83,245.00**

Training		Price	Qty	Ext. Price
uusv-01-ssc-8500	**1 Week Comprehensive SonicWALL Instructor Led Admin Training- 1 Seat**	$4,790.00	3	$14,370.00
		Training Subtotal		**$14,370.00**

Services		Price	Qty	Ext. Price
sssv-gtcntrctinstall	**Professional Services** Estimated Deployment & Optimization Services	$8,750.00	1	$8,750.00
		Services Subtotal		**$8,750.00**

Discount		Price	Qty	Ext. Price
Discount	**Final Discount**	($32,600.00)	1	($32,600.00)
		Discount Subtotal		**($32,600.00)**

Quote Summary	Amount
Hardware	$83,245.00
Training	$14,370.00
Services	$8,750.00
Discount	($32,600.00)
Total	**$73,765.00**

Thank you for allowing Sanity Solutions, Inc. the opportunity to earn your business. By approving this document customer acknowledges configuration and agrees to Sanity Solutions, Inc. Terms and Conditions http://www.sanitysolutions.com/about/terms-and-conditions. Shipping and Sales Tax not included, unless indicated above. Sanity Solutions, Inc. reserves the right to cancel orders arising from pricing or product discrepancies.

Signature _____ Date _____

	9200	9400	9600	9800
Operating system	SonicOS			
Security Processing Cores	24	32		64
10 GbE interfaces	4 x 10-GbE SFP+			
1 GbE interfaces	8 x 1-GbE SFP, 8 x 1 GbE (1 LAN Bypass pair)			12 x 1-GbE SFP, 8 x 1 GbE
Management interfaces	1 GbE, 1 Console			
Memory (RAM)	8 GB	16 GB	32 GB	64 GB
Storage	Flash			2x 80GB SSD, Flash
Expansion	1 Expansion Slot (Rear)*, SD Card*			
Firewall inspection throughput[1]	15 Gbps	20 Gbps		40 Gbps
Application inspection throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
IPS throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
Anti-malware inspection throughput[2]	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps
IMIX performance	4.4 Gbps	5.5 Gbps		9 Gbps
SSL-DPI	1 Gbps	2 Gbps	2 Gbps	5 Gbps
VPN throughput[3]	5 Gbps	10 Gbps	11.5 Gbps	18 Gbps
Latency	17µs			
Connections per second	100,000/sec	130,000/sec		280,000/sec
Maximum connections (SPI)	1.25 M		1.5 M	3 M
Maximum connections (DPI)	1 M		1.25 M	2.5 M
SSO User	80,000	90,000	100,000	110,000
SonicPoints Supported (max)	128			-
VPN	**9200**	**9400**	**9600**	**9800**
Site-to-site tunnels	10,000			25,000
IPSec VPN clients (max)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)	2,000 (10,000)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF			
Networking	**9200**	**9400**	**9600**	**9800**
IP address assignment	Static, DHCP, PPPoE, L2TP and PPTP client, Internal DHCP server, DHCP Relay[4], Internal DHCP server, DHCP Relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT, transparent mode			
VLAN interfaces	512			
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, terminal services[5], Citrix[5]			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications	ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, CSfC, USGv6			
Certifications pending	FIPS 140-2, Common Criteria NDPP, ICSA Anti-Virus, UC-APL			
Hardware	**9200**	**9400**	**9600**	**9800**
Power supply	Dual, redundant, hot swappable, 300 W			Dual, redundant, hot swappable, 500 W
Fans	Dual, redundant, hot swappable			
Display	Front LED display			
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	200			350
MTBF @25°C in Hours	188,719	187,702	186,451	126,144
MTBF @25°C in Years	21.543	21.427	21.284	14.400
Form factor	1U Rack Mountable			2U Rack Mountable
Dimensions	17x19.1x1.75 in (43.3x48.5x4.5 cm)			17x24x3.5 in (9x60x43 cm)
Weight	18.1 lb (8.2 kg)			40.5 lb (18.38 kg)
WEEE weight	23 lb (10.4 kg)			49.5 lb (22.4 kg)
Shipping weight	29.3 lb (13.3 kg)			65 lb (29.64 kg)
Major regulatory	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE , ANATEL, BSMI			
Environment	32-105 F, 0-40 deg C			15-40 deg C
Humidity	10-90% non-condensing			

Request for Proposal
RFP-4089-15-NJ

REPLACEMENT FIREWALL

RESPONSES DUE:
September 30, 2015 prior to 3:30 PM Local

Accepting Electronic Responses Only
Responses Only Submitted Through the Rocky Mountain E-Purchasing System (RMEPS)
https://www.rockymountainbidsystem.com/default.asp
(Purchasing Representative does not have access or control of the vendor side of RMEPS. If website or other problems arise during response submission, vendor MUST contact RMEPS to resolve issue prior to the response deadline. 800-835-4603)

PURCHASING REPRESENTATIVE:
Nicholas C Jones, Buyer
Nickj@gjcity.org
970-244-1533

This solicitation has been developed specifically for a Request for Proposal intended to solicit competitive responses for this solicitation, and may not be the same as previous City of Grand Junction/Mesa County solicitations. All offerors are urged to thoroughly review this solicitation prior to submitting. Submittal by **FAX, EMAIL, or HARD COPY IS NOT ACCEPTABLE** for this solicitation.

REQUEST FOR PROPOSAL

TABLE OF CONTENTS

Section

REQUEST FOR PROPOSAL

SECTION 1.0: ADMINISTRATIVE INFORMATION & CONDITIONS FOR SUBMITTAL

1.1 Issuing Office: This Request for Proposal (RFP) is issued for the City of Grand Junction (Owner) on behalf of the Information Technology Division. All contact regarding this RFP is directed to:

RFP Questions:
Nicholas C Jones, Buyer
Nickj@gjcity.org

1.2 Purpose: The purpose of this RFP is to obtain proposals from qualified professional firms to provide all labor, equipment, and materials required to replace a pair Juniper SSG320 Firewall and a Juniper SA2500 SSL VPN Appliance that have reached End-of-Life for the city.

1.3 The Owner: The Owner is the City of Grand Junction, Colorado and is referred to throughout this Solicitation. The term Owner means the Owner or his authorized representative.

1.4 Mandatory Pre-Proposal Conference: A **mandatory** pre-proposal conference is required for all prospective offerors. The purpose of this visit will be to inspect and to clarify the contents of this Request for Proposal (RFP). Meeting location shall be via online meeting software on **September 9, 2015 at 9:00 AM MDT**. **Pre-Registration is required.** Contact the Purchasing Representative to pre-register for the conference and obtain web-links and information pertaining to the meeting.

1.5 Compliance: All participating Offerors, by their signature hereunder, shall agree to comply with all conditions, requirements, and instructions of this RFP as stated or implied herein. Should the Owner omit anything from this packet which is necessary to the clear understanding of the requirements, or should it appear that various instructions are in conflict, the Offeror(s) shall secure instructions from the Purchasing Division prior to the date and time of the submittal deadline shown in this RFP.

1.6 Submission: Please refer to section 5.0 for what is to be included. ***Each proposal shall be submitted in electronic format only, and only through the Rocky Mountain E-Purchasing website (https://www.rockymountainbidsystem.com/default.asp).*** *This site offers both "free" and "paying" registration options that allow for full access of the Owner's documents and for electronic submission of proposals. (Note: "free" registration may take up to 24 hours to process. Please Plan accordingly.)* Please view our "**Electronic Vendor Registration Guide"** at http://www.gjcity.org/BidOpenings.aspx for details. For proper comparison and evaluation, the City requests that proposals be formatted as directed in Section 5.0 "Preparation and Submittal of Proposals." Submittals received that fail to follow this format may be ruled non-responsive. (Purchasing Representative does not have access or control of the vendor side of RMEPS. If website or other problems arise during response submission, vendor **MUST** contact RMEPS to resolve issue prior to the response deadline. **800-835-4603**)

1.7 Altering Proposals: Any alterations made prior to opening date and time must be initialed by the signer of the proposal, guaranteeing authenticity. Proposals cannot be altered or amended after submission deadline.

1.8 Withdrawal of Proposal: A proposal must be firm and valid for award and may not be withdrawn or canceled by the Offeror prior to the sixty-first (61st) day following the submittal deadline date and only prior to award. The Offeror so agrees upon submittal of their proposal. After award this statement is not applicable.

1.9 Acceptance of Proposal Content: The contents of the proposal of the successful Offeror shall become contractual obligations if acquisition action ensues. Failure of the successful Offeror to accept these obligations in a contract shall result in cancellation of the award and such vendor shall be removed from future solicitations.

1.10 Exclusion: No oral, telegraphic, or telephonic proposals shall be considered.

1.11 Addenda: All Questions shall be submitted in writing to the appropriate person as shown in Section 1.1. Any interpretations, corrections and changes to this RFP or extensions to the opening/receipt date shall be made by a written Addendum to the RFP by the City Purchasing Division. Sole authority to authorize addenda shall be vested in the City of Grand Junction Purchasing Representative. Addenda will be issued electronically through the Rocky Mountain E-Purchasing website at www.rockymountainbidsystem.com. Offerors shall acknowledge receipt of all addenda in their proposal.

1.12 Exceptions and Substitutions: All proposals meeting the intent of this RFP shall be considered for award. Offerors taking exception to the specifications shall do so at their own risk. The Owner reserves the right to accept or reject any or all substitutions or alternatives. When offering substitutions and/or alternatives, Offeror must state these exceptions in the section pertaining to that area. Exception/substitution, if accepted, must meet or exceed the stated intent and/or specifications. The absence of such a list shall indicate that the Offeror has not taken exceptions, and if awarded a contract, shall hold the Offeror responsible to perform in strict accordance with the specifications or scope of work contained herein.

1.13 Confidential Material: All materials submitted in response to this RFP shall ultimately become public record and shall be subject to inspection after contract award. **"Proprietary or Confidential Information"** is defined as any information that is not generally known to competitors and which provides a competitive advantage. Unrestricted disclosure of proprietary information places it in the public domain. Only submittal information clearly identified with the words "***Confidential Disclosure***" and uploaded as a separate document shall establish a confidential, proprietary relationship. Any material to be treated as confidential or proprietary in nature must include a justification for the request. The request shall be reviewed and either approved or denied by the Purchasing Supervisor. If denied, the proposer shall have the opportunity to withdraw its entire proposal, or to remove the confidential or proprietary restrictions. Neither cost nor pricing information nor the total proposal shall be considered confidential or proprietary.

1.14 Response Material Ownership: All proposals become the property of the Owner upon receipt and shall only be returned to the proposer at the Owner's option. Selection or rejection of the proposal shall not affect this right. The Owner shall have the right to use all ideas or adaptations of the ideas contained in any proposal received in response to this RFP, subject to limitations outlined in the section 1.12 entitled "Confidential Material". Disqualification of a proposal does not eliminate this right.

1.15 Minimal Standards for Responsible Prospective Offerors: A prospective Offeror must affirmably demonstrate their responsibility. A prospective Offeror must meet the following requirements:

- Have adequate financial resources, or the ability to obtain such resources as required.
- Be able to comply with the required or proposed completion schedule.
- Have a satisfactory record of performance.
- Have a satisfactory record of integrity and ethics.
- Be otherwise qualified and eligible to receive an award and enter into a contract with the Owner.

1.16 Open Records: Proposals shall be received and publicly acknowledged at the location, date, and time stated herein. Offerors, their representatives and interested persons may be present. Proposals shall be received and acknowledged only so as to avoid disclosure of process. However, all proposals shall be open for public inspection after the contract is awarded. Trade secrets and confidential information contained in the proposal so identified by offer as such shall be treated as confidential by the Owner to the extent allowable in the Open Records Act.

1.17 Sales Tax: City of Grand Junction/Mesa County is, by statute, exempt from the State Sales Tax and Federal Excise Tax; therefore, all fees shall not include taxes.

1.18 Public Opening: Proposals shall be opened in the City Hall Auditorium, 250 North 5th Street, Grand Junction, CO 81501, immediately following the proposal deadline. Offerors, their representatives and interested persons may be present. Only the names and locations on the proposing firms will be disclosed.

SECTION 2.0: GENERAL CONTRACT TERMS AND CONDITIONS

2.1. Acceptance of RFP Terms: A proposal submitted in response to this RFP shall constitute a binding offer. Acknowledgment of this condition shall be indicated on the Letter of Interest or Cover Letter by the autographic signature of the Offeror or an officer of the Offeror legally authorized to execute contractual obligations. A submission in response to the RFP acknowledges acceptance by the Offeror of all terms and conditions including compensation, as set forth herein. An Offeror shall identify clearly and thoroughly any variations between its proposal and the Owner's RFP requirements. Failure to do so shall be deemed a waiver of any rights to subsequently modify the terms of performance, except as outlined or specified in the RFP.

2.2. Execution, Correlation, Intent, and Interpretations: The Contract Documents shall be signed in not less than triplicate by the Owner (Owner) and Contractor. Owner will

provide the contract. By executing the contract, the Contractor represents that he/she has visited the site, familiarized himself with the local conditions under which the Work is to be performed, and correlated his observations with the requirements of the Contract Documents. The Contract Documents are complementary, and what is required by any one, shall be as binding as if required by all. The intention of the documents is to include all labor, materials, equipment and other items necessary for the proper execution and completion of the scope of work as defined in the technical specifications and drawings contained herein. All drawings, specifications and copies furnished by the Owner are, and shall remain, Owner property. They are not to be used on any other project, and with the exception of one contract set for each party to the contract, are to be returned to the owner on request at the completion of the work.

2.3. Permits, Fees, & Notices: The Contractor shall secure and pay for all permits, governmental fees and licenses necessary for the proper execution and completion of the work. The Contractor shall give all notices and comply with all laws, ordinances, rules, regulations and orders of any public authority bearing on the performance of the work. If the Contractor observes that any of the Contract Documents are at variance in any respect, he shall promptly notify the Owner in writing, and any necessary changes shall be adjusted by approximate modification. If the Contractor performs any work knowing it to be contrary to such laws, ordinances, rules and regulations, and without such notice to the Owner, he shall assume full responsibility and shall bear all costs attributable.

2.4. Responsibility for those Performing the Work: The Contractor shall be responsible to the Owner for the acts and omissions of all his employees and all other persons performing any of the work under a contract with the Contractor.

2.5. Use of the Site: The Contractor shall confine operations at the site to areas permitted by law, ordinances, permits and the Contract Documents, and shall not unreasonably encumber the site with any materials or equipment.

2.6. Cleanup: The Contractor at all times shall keep the premises free from accumulation of waste materials or rubbish caused by his operations. At the completion of work he shall remove all his waste materials and rubbish from and about the project, as well as all his equipment and surplus materials.

2.7. Payment & Completion: The Contract Sum is stated in the Contract and is the total amount payable by the Owner to the Contractor for the performance of the work under the Contract Documents. Upon receipt of written notice that the work is ready for final inspection and acceptance and upon receipt of application for payment, the Owner's Project Manager will promptly make such inspection and, when he finds the work acceptable under the Contract Documents and the Contract fully performed, the Owner shall make payment in the manner provided in the Contract Documents. Partial payments will be based upon estimates, prepared by the Contractor, of the value of Work performed and materials placed in accordance with the Contract Documents.

2.8. Protection of Persons & Property: The Contractor shall comply with all applicable laws, ordinances, rules, regulations and orders of any public authority having jurisdiction for the safety of persons or property or to protect them from damage, injury or loss. He shall erect and maintain, as required by existing safeguards for safety and protection, and

all reasonable precautions, including posting danger signs or other warnings against hazards promulgating safety regulations and notifying owners and users of adjacent utilities. When or where any direct or indirect damage or injury is done to public or private property by or on account of any act, omission, neglect, or misconduct by the Contractor in the execution of the work, or in consequence of the non-execution thereof by the Contractor, he shall restore, at his own expense, such property to a condition similar or equal to that existing before such damage or injury was done, by repairing, rebuilding, or otherwise restoring as may be directed, or it shall make good such damage or injury in an acceptable manner.

2.9. Changes in the Work: The Owner, without invalidating the contract, may order changes in the work within the general scope of the contract consisting of additions, deletions or other revisions. All such changes in the work shall be authorized by Change Order and shall be executed under the applicable conditions of the contract documents. A Change Order is a written order to the Contractor signed by the Owner issued after the execution of the contract, authorizing a change in the work or an adjustment in the contract sum or the contract time.

2.10. Minor Changes in the Work: The Owner shall have authority to order minor changes in the work not involving an adjustment in the contract sum or an extension of the contract time and not inconsistent with the intent of the contract documents.

2.11. Uncovering & Correction of Work: The Contractor shall promptly correct all work found by the Owner as defective or as failing to conform to the contract documents. The Contractor shall bear all costs of correcting such rejected work, including the cost of the Owner's additional services thereby made necessary. The Owner shall give such notice promptly after discover of condition. All such defective or non-conforming work under the above paragraphs shall be removed from the site where necessary and the work shall be corrected to comply with the contract documents without cost to the Owner.

2.12. Amendment: No oral statement of any person shall modify or otherwise change, or affect the terms, conditions or specifications stated in the resulting contract. All amendments to the contract shall be made in writing by the Owner Purchasing Division.

2.13. Assignment: The Offeror shall not sell, assign, transfer or convey any contract resulting from this RFP, in whole or in part, without the prior written approval from the Owner.

2.14. Compliance with Laws: Proposals must comply with all Federal, State, County and local laws governing or covering this type of service and the fulfillment of all ADA (Americans with Disabilities Act) requirements.

2.15. Confidentiality: All information disclosed by the Owner to the Offeror for the purpose of the work to be done or information that comes to the attention of the Offeror during the course of performing such work is to be kept strictly confidential.

2.16. Conflict of Interest: No public official and/or Owner employee shall have interest in any contract resulting from this RFP.

2.17. Contract: This Request for Proposal, submitted documents, and any negotiations, when properly accepted by the Owner, shall constitute a contract equally binding between the Owner and Offeror. The contract represents the entire and integrated agreement between the parties hereto and supersedes all prior negotiations, representations, or agreements, either written or oral, including the Proposal documents. The contract may be amended or modified with Change Orders, Field Orders, or Addendums.

2.18. Project Manager/Administrator: The Project Manager, on behalf of the Owner, shall render decisions in a timely manner pertaining to the work proposed or performed by the Offeror. The Project Manager shall be responsible for approval and/or acceptance of any related performance of the Scope of Services.

2.19. Contract Termination: This contract shall remain in effect until any of the following occurs: (1) contract expires; (2) completion of services; (3) acceptance of services or, (4) for convenience terminated by either party with a written *Notice of Cancellation* stating therein the reasons for such cancellation and the effective date of cancellation at least thirty days past notification.

2.20. Employment Discrimination: During the performance of any services per agreement with the Owner, the Offeror, by submitting a Proposal, agrees to the following conditions:

2.20.1. The Offeror shall not discriminate against any employee or applicant for employment because of race, religion, color, sex, age, disability, citizenship status, marital status, veteran status, sexual orientation, national origin, or any legally protected status except when such condition is a legitimate occupational qualification reasonably necessary for the normal operations of the Offeror. The Offeror agrees to post in conspicuous places, visible to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

2.20.2. The Offeror, in all solicitations or advertisements for employees placed by or on behalf of the Offeror, shall state that such Offeror is an Equal Opportunity Employer.

2.20.3. Notices, advertisements, and solicitations placed in accordance with federal law, rule, or regulation shall be deemed sufficient for the purpose of meeting the requirements of this section.

2.21. Immigration Reform and Control Act of 1986 and Immigration Compliance: The Offeror certifies that it does not and will not during the performance of the contract employ illegal alien workers or otherwise violate the provisions of the Federal Immigration Reform and Control Act of 1986 and/or the immigration compliance requirements of State of Colorado C.R.S. § 8-17.5-101, *et.seq.* (House Bill 06-1343).

2.22. Ethics: The Offeror shall not accept or offer gifts or anything of value nor enter into any business arrangement with any employee, official, or agent of the Owner.

2.23. Failure to Deliver: In the event of failure of the Offeror to deliver services in accordance with the contract terms and conditions, the Owner, after due oral or written notice, may procure the services from other sources and hold the Offeror responsible for any costs

resulting in additional purchase and administrative services. This remedy shall be in addition to any other remedies that the Owner may have.

2.24. Failure to Enforce: Failure by the Owner at any time to enforce the provisions of the contract shall not be construed as a waiver of any such provisions. Such failure to enforce shall not affect the validity of the contract or any part thereof or the right of the Owner to enforce any provision at any time in accordance with its terms.

2.25. Force Majeure: The Offeror shall not be held responsible for failure to perform the duties and responsibilities imposed by the contract due to legal strikes, fires, riots, rebellions, and acts of God beyond the control of the Offeror, unless otherwise specified in the contract.

2.26. Indemnification: Offeror shall defend, indemnify and save harmless the Owner, State of Colorado, and all its officers, employees, insurers, and self-insurance pool, from and against all liability, suits, actions, or other claims of any character, name and description brought for or on account of any injuries or damages received or sustained by any person, persons, or property on account of any negligent act or fault of the Offeror, or of any Offeror's agent, employee, subcontractor or supplier in the execution of, or performance under, any contract which may result from proposal award. Offeror shall pay any judgment with cost which may be obtained against the Owner growing out of such injury or damages.

2.27. Independent Firm: The Offeror shall be legally considered an Independent Firm and neither the Firm nor its employees shall, under any circumstances, be considered servants or agents of the Owner. The Owner shall be at no time legally responsible for any negligence or other wrongdoing by the Firm, its servants, or agents. The Owner shall not withhold from the contract payments to the Firm any federal or state unemployment taxes, federal or state income taxes, Social Security Tax or any other amounts for benefits to the Firm. Further, the Owner shall not provide to the Firm any insurance coverage or other benefits, including Workers' Compensation, normally provided by the Owner for its employees.

2.28. Nonconforming Terms and Conditions: A proposal that includes terms and conditions that do not conform to the terms and conditions of this Request for Proposal is subject to rejection as non-responsive. The Owner reserves the right to permit the Offeror to withdraw nonconforming terms and conditions from its proposal prior to a determination by the Owner of non-responsiveness based on the submission of nonconforming terms and conditions.

2.29. Ownership: All plans, prints, designs, concepts, etc., shall become the property of the Owner.

2.30. Oral Statements: No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in this document and/or resulting agreement. All modifications to this request and any agreement must be made in writing by the Owner.

2.31. Patents/Copyrights: The Offeror agrees to protect the Owner from any claims involving infringements of patents and/or copyrights. In no event shall the Owner be liable to the Offeror for any/all suits arising on the grounds of patent(s)/copyright(s) infringement. Patent/copyright infringement shall null and void any agreement resulting from response to this RFP.

2.32. Remedies: The Offeror and Owner agree that both parties have all rights, duties, and remedies available as stated in the Uniform Commercial Code.

2.33. Venue: Any agreement as a result of responding to this RFP shall be deemed to have been made in, and shall be construed and interpreted in accordance with, the laws of the City of Grand Junction, Mesa County, Colorado.

2.34. Expenses: Expenses incurred in preparation, submission and presentation of this RFP are the responsibility of the company and can not be charged to the Owner.

2.35. Sovereign Immunity: The Owner specifically reserves its right to sovereign immunity pursuant to Colorado State Law as a defense to any action arising in conjunction to this agreement.

2.36. Public Funds/Non-Appropriation of Funds: Funds for payment have been provided through the City of Grand Junction/Mesa County budget approved by the City Council/Board of County Commissioners for the stated fiscal year only. State of Colorado statutes prohibit the obligation and expenditure of public funds beyond the fiscal year for which a budget has been approved. Therefore, anticipated orders or other obligations that may arise past the end of the stated City of Grand Junction/Mesa County fiscal year shall be subject to budget approval. Any contract will be subject to and must contain a governmental non-appropriation of funds clause.

2.37. Collusion Clause: Each Offeror by submitting a proposal certifies that it is not party to any collusive action or any action that may be in violation of the Sherman Antitrust Act. Any and all proposals shall be rejected if there is evidence or reason for believing that collusion exists among the proposers. The Owner may or may not, at the discretion of the Owner Purchasing Representative, accept future proposals for the same service or commodities for participants in such collusion.

2.38. Gratuities: The proposer certifies and agrees that no gratuities, kickbacks or contingency fees were paid in connection with this contract, nor were any fees, commissions, gifts or other considerations made contingent upon the award of this contract. If the proposer breaches or violates this warranty, the Owner may, at their discretion, terminate this contract without liability to the Owner.

2.39. Safety Warranty: Offeror also warrants that the services performed shall conform to the standards declared by the US Department of Labor under the Occupational Safety and Health Act of 1970.

2.40. OSHA Standards: All Offerors agree and warrant that services performed in response to this invitation shall conform to the standards declared by the US Department of Labor under the Occupational Safety and Health Act of 1970 (OSHA). In the event the services

do not conform to OSHA Standards, the Owner may require the services to be redone at no additional expense to the Owner.

2.41. Performance of the Contract: The Owner reserves the right to enforce the performance of the contract in any manner prescribed by law or deemed to be in the best interest of the Owner in the event of breach or default of resulting contract award.

2.42. Benefit Claims: The Owner shall not provide to the Offeror any insurance coverage or other benefits, including Worker's Compensation, normally provided by the Owner for its employees.

2.43. Default: The Owner reserves the right to terminate the contract immediately in the event the Offeror fails to meet delivery or completion schedules, or otherwise perform in accordance with the accepted proposal. Breach of contract or default authorizes the Owner to purchase like services elsewhere and charge the full increase in cost to the defaulting Offeror.

2.44. Multiple Offers: Proposers must determine for themselves which product to offer. If said proposer chooses to submit more than one offer, THE ALTERNATE OFFER must be clearly marked "Alternate Proposal". The Owner reserves the right to make award in the best interest of the Owner.

2.45. Cooperative Purchasing: Purchases as a result of this solicitation are primarily for the Owner. Other governmental entities may be extended the opportunity to utilize the resultant contract award with the agreement of the successful provider and the participating agencies. All participating entities will be required to abide by the specifications, terms, conditions and pricings established in this Proposal. The quantities furnished in this proposal document are for only the Owner. It does not include quantities for any other jurisdiction. The Owner will be responsible only for the award for our jurisdiction. Other participating entities will place their own awards on their respective Purchase Orders through their purchasing office or use their purchasing card for purchase/payment as authorized or agreed upon between the provider and the individual entity. The Owner accepts no liability for payment of orders placed by other participating jurisdictions that choose to piggy-back on our solicitation. Orders placed by participating jurisdictions under the terms of this solicitation will indicate their specific delivery and invoicing instructions.

2.46. Definitions:

2.46.1. "Consultant" refers to the person, partnership, firm or corporation entering into an Agreement with the Owner for the services required and the legal representatives of said party or the agent appointed to act for said party in the performance of the service(s) contracted for.

2.46.2. "Offeror" refers to the person or persons legally authorized by the Consultant to make an offer and/or submit a response (fee) proposal in response to the Owner's RFP.

2.46.3. The term "Work" includes all labor necessary to produce the requirements by the Contract Documents, and all materials and equipment incorporated or to be incorporated in such construction.

2.46.4. "Owner" is the City of Grand Junction/Mesa County, Colorado and is referred to throughout the Contract Documents. The term Owner means the Owner or his authorized representative. The Owner shall, at all times, have access to the work wherever it is in preparation and progress. The Contractor shall provide facilities for such access. The Owner will make periodic visits to the site to familiarize himself generally with the progress and quality of work and to determine, in general, if the work is proceeding in accordance with the contract documents. Based on such observations and the Contractor's Application for Payment, the Owner will determine the amounts owing to the Contractor and will issue Certificates for Payment in such amounts, as provided in the contract. The Owner will have authority to reject work which does not conform to the Contract documents. Whenever, in his reasonable opinion, he considers it necessary or advisable to insure the proper implementation of the intent of the Contract Documents, he will have authority to require the Contractor to stop the work or any portion, or to require special inspection or testing of the work, whether or not such work can be then be fabricated, installed, or completed. The Owner will not be responsible for the acts or omissions of the Contractor, and sub-Contractor, or any of their agents or employees, or any other persons performing any of the work.

2.46.5. "Contractor is the person or organization identified as such in the Agreement and is referred to throughout the Contract Documents. The term Contractor means the Contractor or his authorized representative. The Contractor shall carefully study and compare the General Contract Conditions of the Contract, Specification and Drawings, Scope of Work, Addenda and Modifications and shall at once report to the Owner any error, inconsistency or omission he may discover. Contractor shall not be liable to the Owner for any damage resulting from such errors, inconsistencies or omissions. The Contractor shall not commence work without clarifying Drawings, Specifications, or Interpretations.

2.46.6. "Sub-Contractor is a person or organization who has a direct contract with the Contractor to perform any of the work at the site. The term sub-contractor is referred to throughout the contract documents and means a sub-contractor or his authorized representative.

2.47. Public Disclosure Record: If the Proposer has knowledge of their employee(s) or sub-proposers having an immediate family relationship with a Owner employee or elected official, the proposer must provide the Purchasing Representative with the name(s) of these individuals. These individuals are required to file an acceptable "Public Disclosure Record", a statement of financial interest, before conducting business with the Owner.

2.48. Keep Jobs in Colorado Act: Contractor shall be responsible for ensuring compliance with Article 17 of Title 8, Colorado Revised Statutes requiring 80% Colorado labor to be employed on public works. Contractor shall, upon reasonable notice provided by the Owner, permit the Owner to inspect documentation of identification and residency required by C.R.S. §8-17-101(2)(a). If Contractor claims it is entitled to a waiver pursuant to C.R.S. §8-17-101(1), Contractor shall state that there is insufficient Colorado labor to perform the work such that compliance with Article 17 would create an undue burden that would substantially prevent a project from proceeding to completion, and shall include evidence demonstrating the insufficiency and undue burden in its response.

Unless expressly granted a waiver by the Owner pursuant to C.R.S. §8-17-101(1), Contractor shall be responsible for ensuring compliance with Article 17 of Title 8, Colorado Revised Statutes requiring 80% Colorado labor to be employed on public works. Contractor shall, upon reasonable notice provided by the Owner, permit the Owner to inspect documentation of identification and residency required by C.R.S. §8-17-101(2)(a).

2.48.1. "Public project" is defined as:

(a) any construction, alteration, repair, demolition, or improvement of any land, building, structure, facility, road, highway, bridge, or other public improvement suitable for and intended for use in the promotion of the public health, welfare, or safety and any maintenance programs for the upkeep of such projects

(b) for which appropriate or expenditure of moneys may be reasonably expected to be $500,000.00 or more in the aggregate for any fiscal year

(c) except any project that receives federal moneys.

SECTION 3.0: INSURANCE REQUIREMENTS

Insurance Requirements: The selected Firm agrees to procure and maintain, at its own cost, policy(s) of insurance sufficient to insure against all liability, claims, demands, and other obligations assumed by the Firm pursuant to this Section. Such insurance shall be in addition to any other insurance requirements imposed by this Contract or by law. The Firm shall not be relieved of any liability, claims, demands, or other obligations assumed pursuant to this Section by reason of its failure to procure or maintain insurance in sufficient amounts, durations, or types.

Firm shall procure and maintain and, if applicable, shall cause any Subcontractor of the Firm to procure and maintain insurance coverage listed below. Such coverage shall be procured and maintained with forms and insurers acceptable to The Owner. All coverage shall be continuously maintained to cover all liability, claims, demands, and other obligations assumed by the Firm pursuant to this Section. In the case of any claims-made policy, the necessary retroactive dates and extended reporting periods shall be procured to maintain such continuous coverage. Minimum coverage limits shall be as indicated below unless specified otherwise in the Special Conditions:

(a) Worker Compensation insurance to cover obligations imposed by applicable laws for any employee engaged in the performance of work under this Contract, and Employers' Liability insurance with minimum limits of:

FIVE HUNDRED THOUSAND DOLLARS ($500,000) each accident,
FIVE HUNDRED THOUSAND DOLLARS ($500,000) disease - policy limit, and
FIVE HUNDRED THOUSAND DOLLARS ($500,000) disease - each employee

(b) General Liability insurance with minimum combined single limits of:

ONE MILLION DOLLARS ($1,000,000) each occurrence and
ONE MILLION DOLLARS ($1,000,000) per job aggregate.

The policy shall be applicable to all premises and operations. The policy shall include coverage for bodily injury, broad form property damage (including completed operations), personal injury (including coverage for contractual and employee acts), blanket contractual, products, and completed operations. The policy shall include coverage for explosion, collapse, and underground hazards. The policy shall contain a severability of interests provision.

(c) Comprehensive Automobile Liability insurance with minimum combined single limits for bodily injury and property damage of not less than:

ONE MILLION DOLLARS ($1,000,000) each occurrence and
ONE MILLION DOLLARS ($1,000,000) aggregate

This policy shall provide coverage to protect the contractor against liability incurred as a result of the professional services performed as a result of responding to this Solicitation.

With respect to each of Consultant's owned, hired, or non-owned vehicles assigned to be used in performance of the Work. The policy shall contain a severability of interests provision. The policies required by paragraphs (b), and (c) above shall be endorsed to include the Owner and the Owner's officers and employees as additional insureds. Every policy required above shall be primary insurance, and any insurance carried by the Owner, its officers, or its employees, or carried by or provided through any insurance pool of the Owner, shall be excess and not contributory insurance to that provided by Consultant. No additional insured endorsement to any required policy shall contain any exclusion for bodily injury or property damage arising from completed operations. The Consultant shall be solely responsible for any deductible losses under any policy required above.

SECTION 4.0: SPECIFICATIONS/SCOPE OF SERVICES

4.1. General/Background: The City of Grand Junction is soliciting proposals to replace a pair Juniper SSG320 Firewall and a Juniper SA2500 SSL VPN Appliance that have reached End-of-Life for the city.

4.2. Overview of City's Infrastructure related to the project:

4.2.1. **Firewall Environment:** The Juniper SSG320 Firewalls are configured as a Primary device and a warm spare. The Firewall is currently used only as a port filtering device. The Juniper SA2500 is used for remote VPN access into the City's network by city staff and vendors. The VPN is integrated with RSA two-factor authentication.

Untrusted Network Connection: Currently the SSG320 is connected to the network with a 1 GB Base-T connection from the primary internet switch which is connected to a router provided by our internet service provider and a fiber link to Mesa County's network.

Trusted Network Connection: The SSG320 is connected to a Sourcefire SSL decryption appliance which is connected to a Sourcefire 3D8350 IDS/IPS sensor, which is then connected to a Cisco Nexus 7K switch via 1000Base-T connection.

A warm spare is kept updated as modification to the primary system are made so that it can deployed in production if the primary unit fails.

The Firewall fails to a closed state during a system hardware failure.

4.2.2. **SSL VPN Environment:** The SA2500 SSL VPN appliance is connected to the Cisco Nexus 7K switch and services all VPN requests for the untrusted network.

4.2.3. **WebFiltering/Reporting Environment:** A Netspective WebFilter appliance is port mirrored to the Cisco port that the firewall is connected to for monitoring, enforcing and reporting all web activities by internal users and devices. All users are granted access to internet resources based on webfilter policies associated with Microsoft Active Directory (AD) group memberships on a User/Computer authorization basis. One (1) Year of web activity is maintained for reporting purposes and reports are generated automatically daily. Reports are also generate on demand as requested by supervisor and managers.

4.3. Specifications: The city is seeking proposals to replace the Juniper SSG320 firewall and SA2500 SSL VPN appliance with a NextGen Application filtering firewall and SSL VPN device. Depending on the proposed replacement solution, the Netspective Webfiltering/enforcement/Reporting appliances may also be replaced.

4.3.1. **Management Interface Requirement:** The firewall must be capable of being managed via both web based Graphical User Interface (GUI) and Command Line Interface (CLI).

4.3.2. **Technical Support Requirement:** The selected vendor must propose a 24x7 support plan that includes on-site support when necessary.

4.3.3. **RSA Authentication Manager Requirement:** SSL/VPN authentication must support two-factor authentication using RSA Hard and Soft tokens via the RSA Authentication Manager.

4.3.4. **FBI Criminal Justice Information Services (CJIS) Security Policy Requirement:** Firewall and SSL VPN solutions must be compliant with FBI CJIS policies and must maintain compliance via upgrades as the CJIS policy evolves.

4.3.5. **VPN:** VPN must have both client and clientless functionality. VPN clients must support MS Windows, Mac OSX, Apple iOS, and Android based operating systems.

4.3.6. **NIST Certification Encryption Algorithm Requirement:** The CJIS Security Policy requires that all data transmitted outside the boundary of a physically secure location be encrypted using a 128-bit encryption standard certified by the National Institute of Standards and Technology (NIST) to ensure that the

cryptographic modules meet Federal Information Processing Standard (FIPS) 140-2 certification requirements. This certification must be presented to the auditors as part of their periodic CJIS audit.

Please submit a copy of encryption certificates to show compliance with the FBI CJIS Policy.

4.3.7. **Fail Closed Requirement:** The firewall must fail closed during a hardware or software failure. At no time can the firewall or VPN allow communication between the untrusted and trusted networks without the communication passing through an active restrictive rule set.

4.3.8. **Traffic Throttling/Shaping:** The new firewall must be able to throttle network traffic based on: Application Traffic Type (i.e. music streaming, ftp traffic), and network interface (i.e. Interface 1- limited to 5Gb, Interface 2 -- unlimited, Interface 3 -- 500Mb).

4.3.9. **Performance:** Must be able to support up to 500 simulations users of internet resources. The request for services can be from both a trusted to untrusted network or from an untrusted to trusted network.

4.3.10. **Network Traffic Analysis:** Must be able to perform detailed traffic analysis reporting showing potential network issues. This reporting can use Netflow or other tools to capture and report

4.3.11. **Logs:** All system generated logs must meet able to be sent to a centralized Log Management System for Centralized correlation, analysis, and retention independent of the devices' log storage and reporting functions.

4.3.12. **Alerts:** Real-Time Alerts must be configurable to notify administrators of events identified by City policy as critical (i.e., system failure/errors, supplications activity, policy violations….etc.)

4.3.13. **10Gb/1Gb Network Requirement:** The Firewall must be able to support 10Gb and 1Gb network interfaces -- both Base-T or SFP+ (Copper or Fiber) -- to the Cisco Sourcefire 3D8350 Sensor and Network Switches.

4.3.14. **Port and IP Packet Filtering:** Must be able to perform traditional firewall port filtering (Layer 2 & Layer 3). Must be able to support stateful packet filtering.

4.3.15. **NAT and PAT:** Must support both dynamic and static NAT and PAT

4.3.16. **IPv4 and IPv6 Support:** Must be able to fully support all firewall features using IPv4 and IPv6 addressing.

4.3.17. **Applications Filtering:** The solution must use application awareness, full stack visibility and granular control to deny or allow network traffic based on an application's identification or layer. The solution must accommodate known

applications based on security vendor lookup mechanisms and custom applications identified by the City.

4.3.18. **Onsite Configuration and Training Requirement:** Contractor shall propose onsite configuration, setup and knowledge transfer. The solution must include formal classroom style training for a minimum of 3 Staff Members with an option to add up to three additional staff members.

4.3.19. **Access Control Integration with Active Directory:** The system must be configurable to integrate with AD and perform Access Control functions based on User ID and Group Memberships.

4.3.20. **VPN Support:** The solution must support SSL-based VPN and client application based VPN functions for a minimum of 25 simulations connections. User pools for VPN access may be selected from AD or configured as non-AD, local users.

4.3.21. **Redundancy:** The solution must include a redundant capability that ensures that a firewall be available during an outage. The solution may include a fully configured hot or warm spare.

4.3.22. **Optional – Web Content Filtering:** The proposed solution may include an option to replace the Netspective Content Filtering appliances.

If included, the option must be able to use AD to identify, track and report on user activities: internet resources accessed, times and dates accessed, and whether the access was allowed or blocked based on a managed rule set. The proposed option should provide flexible reporting capabilities for usage analysis based on user, website, website categories, and types of traffic.

Computers/Laptops/Tablets/Phones not connected to the City's internal network must also be able to track user activities and report back to a central reporting database when reconnected to either the internal network or the Internet. The proposed solution should be able to enforce selected activities even when the device is not connected to the internal network.

The system should generate daily activity reports that are automatically sent to administrators based on City specified criteria. The reports must be able to be generated on-demand.

Real-time alerts for policy violations should be automatically sent to administrators.

4.3.23. **Reporting:** Must be able to provide customizable detailed and summary based reports. Reports must be able to be scheduled for delivery to administrators and allow on-demand reporting.

4.4. Special Conditions/Provisions:

4.4.1. **Freight/Shipping:** All freight/shipping shall be F.O.B. Destination – Freight Pre-Paid and Allowed to the project site.

4.4.2. **Product/Materials Quantities:** Contractor shall be responsible for determining all measurements for correctness, and all quantities of products/materials required for successful project completion. All measurements and quantities provided by Owner are estimates only.

4.4.3. **Pricing:** Pricing shall be all inclusive to include, but not be limited to: all labor, equipment, supplies, materials, freight (F.O.B. Destination – Freight Pre-paid and Allowed), travel, installation, setup, configuration, training/knowledge transfer, and all other costs related to the successful completion of project.

The Owner shall not pay nor be liable for any other additional costs including but not limited to: taxes, shipping charges, insurance, interest, penalties, termination payments, attorney fees, liquidated damages, etc.

4.4.4. **Location:** The project location will be City of Grand Junction City Hall, 250 N. 5Th Street Grand Junction, CO 81501.

4.5. Mandatory Pre-Proposal Conference: A **mandatory** pre-proposal conference is required for all prospective offerors. The purpose of this visit will be to inspect and to clarify the contents of this Request for Proposal (RFP). Meeting location shall be via online meeting software on **September 9, 2015 at 9:00 AM MDT**. **Pre-Registration is required.** Contact the Purchasing Representative to pre-register for the conference and obtain web-links and information pertaining to the meeting.

4.6. RFP Tentative Time Schedule:

• Request for Proposal available on or before	August 31, 2015
• Mandatory Pre-Proposal Conference	September 9, 2015
• Inquiry deadline, no questions after this date	September 14, 2015
• Addenda Issued by	September 16, 2015
• Submittal deadline for proposals	September 30, 2015
• Owner evaluation of proposals	Late October
• Web Demo/Interviews	Late October

4.7. Questions Regarding Scope of Services:

Nicholas C Jones, Buyer
Nickj@gjcity.org

SECTION 5.0: PREPARATION AND SUBMITTAL OF PROPOSALS

Submission: ***Each proposal shall be submitted in electronic format only, and only through the Rocky Mountain E-Purchasing website (https://www.rockymountainbidsystem.com/default.asp).*** *This site offers both "free" and "paying" registration options that allow for full access of the Owner's documents and for electronic submission of proposals. (Note: "free" registration may take up to 24 hours to process. Please Plan accordingly.)* Please view our **"Electronic Vendor Registration Guide"** at http://www.gjcity.org/BidOpenings.aspx for details. Offerors are required to indicate their interest in this Project, show their specific experience and address their capability to perform the Scope of Services in the Time Schedule as set forth herein. For proper comparison and evaluation, the Owner requires that proposals be formatted **A to H**.

A. Cover Letter: Cover letter shall be provided which explains the Firm's interest in the project. The letter shall contain the name/address/phone number of the person who will serve as the firm's principal contact person with Owner's Contract Administrator and shall identify individual(s) who will be authorized to make presentations on behalf of the firm. The statement shall bear the signature of the person having proper authority to make formal commitments on behalf of the firm. By submitting a response to this solicitation the Contractor agrees to all requirements herein. An acknowledgement of receipt of all Addenda shall also be included.

B. Qualifications/Experience/Credentials: Proposers shall provide their qualifications for consideration as a contract provider to the City of Grand Junction and include prior experience in similar projects.

C. Strategy and Implementation Plan: Describe your (the firm's) interpretation of the Owner's objectives with regard to this RFP. Describe the proposed strategy and/or plan for achieving the objectives of this RFP. The Firm may utilize a written narrative or any other printed technique to demonstrate his/her ability to satisfy the Scope of Services. The narrative should describe a logical progression of tasks and efforts starting with the initial steps or tasks to be accomplished and continuing until all proposed tasks are fully described and the RFP objectives are accomplished. Include a time schedule for completion of your firm's implementation plan and an estimate of time commitments from Owner staff. Please specify any product lead times.

D. References: A minimum of three (3) references with their names, addresses and telephone numbers that can attest to your experience in projects of similar scope and size.

E. Fee Proposal: Provide a complete and detailed list of costs and total project cost. Include subsequent yearly maintenance costs as these will be a factor in the evaluation process.

F. Solicitation Response Form: Provide a completed Solicitation Response Form found in Section 7.0.

G. Warranty: Provide proof of standard manufacturer's warranty as well as optional additional or extended warranties offered. Include manufacturer documentation describing the expected life expectancy of the proposed equipment.

H. Additional Data: Provide any product data sheets and any additional information that will aid in evaluation of your qualifications with respect to this project.

SECTION 6.0: EVALUATION CRITERIA AND FACTORS

6.1 Evaluation: An evaluation team shall review all responses and select the proposal or proposals that best demonstrate the capability in all aspects to perform the scope of services and possess the integrity and reliability that will ensure good faith performance.

6.2 Intent: Only respondents who meet the qualification criteria will be considered. Therefore, it is imperative that the submitted proposal clearly indicate the firm's ability to provide the services described herein.

Submittal evaluations will be done in accordance with the criteria and procedure defined herein. The Owner reserves the right to reject any and all Statements. The following parameters will be used to evaluate the submittals (in no particular order of priority):

- Responsiveness of submittal to the RFP
- Understanding of the project and the objectives
- Necessary resources
- Strategy & Implementation Plan
- Demonstrated capability
- References
- Ongoing Annual Support and Maintenance Costs
- Product Lifecycle and Warranty

The Owner will undertake negotiations with the top rated firm and will not negotiate with lower rated firms unless negotiations with higher rated firms have been unsuccessful and terminated.

6.3 Oral Interviews: The Owner anticipates inviting the most qualified rated proposers to participate in web demo/interviews.

6.4 Award: Firms shall be ranked or disqualified based on the criteria listed in Section 6.2. The Owner reserves the right to consider all of the information submitted and/or oral presentations, if required, in selecting the project Contractor.

SECTION 7.0: SOLICITATION RESPONSE FORM

RFP-4060-15-NJ Replacement Firewall

Offeror must submit entire Form completed, dated and signed.

The Owner reserves the right to accept any portion of the work to be performed at its discretion

---

The undersigned has thoroughly examined the entire Request for Proposals and therefore submits the proposal and schedule of fees and services attached hereto.

This offer is firm and irrevocable for sixty (60) days after the time and date set for receipt of proposals.

The undersigned Offeror agrees to provide services and products in accordance with the terms and conditions contained in this Request for Proposal and as described in the Offeror's proposal attached hereto; as accepted by the Owner.

Prices in the proposal have not knowingly been disclosed with another provider and will not be prior to award.

- Prices in this proposal have been arrived at independently, without consultation, communication or agreement for the purpose of restricting competition.
- No attempt has been made nor will be to induce any other person or firm to submit a proposal for the purpose of restricting competition.
- The individual signing this proposal certifies that he/she is a legal agent of the offeror, authorized to represent the offeror and is legally responsible for the offer with regard to supporting documentation and prices provided.
- Direct purchases by the Owner are tax exempt from Colorado Sales or Use Tax. Tax exempt No. 98-903544. The undersigned certifies that no Federal, State, County or Municipal tax will be added to the above quoted prices.
- Prompt payment discount of _____ percent of the net dollar will be offered to the Owner if the invoice is paid within _____ days after the receipt of the invoice. Payment Terms _____.

RECEIPT OF ADDENDA: the undersigned Contractor acknowledges receipt of Addenda to the Solicitation, Specifications, and other Contract Documents.

State number of Addenda received: _____.

It is the responsibility of the Proposer to ensure all Addenda have been received and acknowledged.

Date: _____

_____	_____
Company Name – (Typed or Printed)	Authorized Agent – (Typed or Printed)
_____	_____
Authorized Agent Signature	Title
_____	_____
Address of Offeror	Owner, State, and Zip Code
_____	_____
Phone Number	E-mail Address of Agent

CITY OF Grand Junction COLORADO

MESA COUNTY

Purchasing Division

ADDENDUM NO. 1

DATE: **September 15, 2015**
FROM: **City of Grand Junction Purchasing Division**
TO: **All Offerors**
RE: **Replacement Firewall RFP-4089-15-NJ**

Offerors responding to the above referenced solicitation are hereby instructed that the requirements have bee n c larified, modified, s uperseded and s upplemented as t o t his date as hereinafter described.

Please make note of the following clarifications:

1. **Question 1:** "Regarding 4.3.13, what port density is required? Specifically how many 10Gb ports are required? On the call the question was asked by me but the answer was 4-6 ports; do you have solid number of ports? This would determine the cost of the product solution we offer."
   Response: Minimum of 3 - 10Gb ports and 4 - 1Gb Ports.

2. **Question 2:** "…is currently in the process of FIPS-140 compliance/certification but we will not have our certificate in time for the response date. Is this a 100% requirement? In other words, will my response be disqualified if I don't have a certificate in my response?"
   Response: The certification/compliance is a requirement. The Owner will consider solutions if the contractor can be certified by award dates.

The original solicitation for the project noted above is amended as noted.

All other conditions of subject remain the same.

Respectfully,

Nicholas C Jones, Buyer
City of Grand Junction, Colorado

Cover Letter

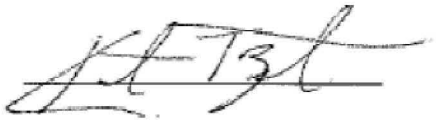
Sanity Solutions has partnered with Dell to deliver the following response to City of Grand Junction's current Replacement Firewall Request for Proposal. Our strategic partnership allows us to provide our customers with a very dedicated local team of experts working together to architect and deploy solutions built on market leading hardware and software closely following industry standards and best practices. Mutual customers appreciate the extensive expertise, service and value our local account teams provide their organizations.

This turn-key solution will replace the existing Juniper appliances with the latest technologies from Dell SonicWALL, a long time industry leader in firewall and comprehensive security offerings. This solution meets all required criteria and is future-proof with the right amount of room to grow with exceptional agility and a low, predictable TCO over the life of the platform. Our goal was to design a solution that is highly tailored to the projects specific requirements identified in the request, while also providing thoughtfulness and additional resources for increasing overall security posture across the entire organization moving forward.

Sanity Solutions and Dell both appreciate their longtime partnerships with the City of Grand Junction, we welcome the opportunity to work together on this important project and see it through to successful completion.

Sanity Solutions and Dell agree to and adhere by all requirements in the Request for Proposal document RFP-4089-15-NJ. All persons below are authorized to present on behalf of their respective organizations with regards to this proposal.

Sincerely,



Keith T. Barnholt
Account Executive
Sanity Solutions
720-289-3029
KBarnholt@sanitysolutions.com
1720 S. Bellaire St. Suite 550
Denver, CO 80222

David Stalcup
Principal Storage Architect
Sanity Solutions

Ryan Hayes
Sr. Engineer, Security Specialist
Sanity Solutions

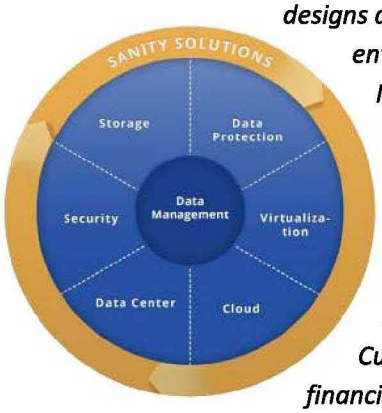
Jessica Engar
Regional SonicWALL Sales Manager
Dell

Adam Zimmerer
Sr. SonicWALL Engineer
Dell

Qualifications/Experience/Credentials

Company Profile

***Sanity Solutions, Inc**. is headquartered in Denver, Colorado with offices throughout the country. Sanity designs and deploys holistic data management solutions for a variety of State & Local entities, School Districts, Federal Government Agencies, Hospitals, Educational Institutions, Small/Medium Businesses and Enterprises across the world.*



Sanity Solutions is partnered with over 20 vendors covering technologies in storage, servers, networking, data protection, virtualization, data security, cloud computing and data center power & cooling. The sales and technical teams engage closely with IT departments to design solutions built on leading technologies that closely follow industry standards and best practices. Customers of Sanity consistently achieve their technical, operational and financial goals.

At Sanity's national headquarters in Denver just north of the Tech Center, their team frequently hosts customer project meetings, executive briefings, free educational events and run demos from their Test Lab. The Sanity Test Lab hosts Dell Compellent, EqualLogic, and PowerVault Storage Arrays, Nexsan Storage, Dell Servers (11/12/13G), Dell VRTX and FX2 Converged Platforms, Dell Networking & Cisco Switches, SonicWALL Next Gen Firewall, VMware, CommVault, Veeam, and Actifio.

Sanity Solutions' Engineering and Professional Services Staff is consistently recognized by CRN Magazine as one of the nation's most technically certified teams and among the industry's elite. Their specialties include- Infrastructure Design, Installation & Deployment, Critical Application Optimization, Migration Services, Health Monitoring, System Diagnostics & Reporting and Topic Specific Consulting. All Engineers and Architects have reached the highest levels of certification across all of their strategic partnerships.

Sanity Solutions is an elite Dell Premier Partner. Out of over 25,000 Dell resellers worldwide, there are less than 200 Premier resellers, putting Sanity in the top 1%. Also recognized as a National DoMore Partner, they are one of the top-rated integrators among this elite 1% of global partners. The account teams design and deploy comprehensive solutions across all of Dell's lines of business from the core of the data center to the end user interface.

Sanity was recently recognized for the second year in a row as Dell's Partner of the Year for the West and South Central Regions of the U.S. This recognition is based on a number of factors including breadth of technical and sales expertise, quality of professional service performed, performance and standing amongst peers, and the overall quality of service and additional value provided to their customers.

Sanity Solutions Named Dell PartnerDirect West Partner of the Year

As IT moves from being the backbone of business to being the business, customers' IT must enable faster, more secure access to information, modern software and applications, as well as optimize workloads and ensure the business is competitive. For all of these reasons and more, Sanity Solutions chooses Dell to provide products that are easy to use, manage and scale at an affordable price. As Dell has grown, and continues to grow, their dynamic product offering, they have remain focused on the needs of the customers, large or small. As Dell and Sanity look toward the future, we can collaboratively assist our customers with their next generation virtualized data center needs.

Sanity Solutions receiving Dell Partner of the Year Award

This annual award honors Dell Partners for delivering exemplary solutions and superior level of expertise for their customers during the past year. Selected from 146,000 Dell partners worldwide, Sanity Solutions received this award based on dedicated use of Dell technologies to extend and enhance Dell's reach and power to do more for customers.

"I'm thrilled to congratulate Sanity Solutions on being named a Dell Partner of the Year, when companies decide to move forward with a technology purchase, one of the biggest considerations is who to work with to help them through the process, educate their team, review financing options, recommend the best products and solutions, and put together a comprehensive package that fits their budget. Customers can be assured that as a Dell Premier Partner, Sanity Solutions is a trusted advisor ready to help them choose the best solution for their IT challenges."

– **Frank Vitagliano**
Vice President of Channel Sales at Dell

"Through the development of great relationships and true partnering, Sanity has continued to invest and grow their Dell business over 40% for the last two years."

– **Paul Casanova, Dell Channel Manager**

Strategic Partnerships

Industry Recognition

Corporate Profile

***Dell** is a global information technology company that offers its customers a broad range of solutions and services. The company was founded in 1984 in Austin, TX where they are still headquartered. With over 110,000 employees worldwide, Dell connects with more than 5.4 million customers every day. They are focused on providing technology solutions that are efficient, accessible and easy to manage. They have operations and conduct business in three geographic regions:*

- *The Americas region, based in Round Rock, Texas, covers the US, Canada and Latin America*
- *The EMEA region, based in Bracknell, England, covers Europe, the Middle East and Africa*
- *The APJ region, based in Singapore, covers the Asian countries of the Pacific Rim, Australia, New Zealand and India*

They have more than 43,000 Services team members in approximately 90 countries, 60 technical support centers and seven global command centers dedicated to helping customers use technology to reach their business goals.

Within the last few years Dell has also become a leading end-to-end technology solutions company. Their enterprise solutions include servers, networking, and storage offerings. In services, they provide end-to-end technology solutions to their customers, including managed security services focused on threat intelligence and security consulting. Their services include a broad range of configurable IT and business services, including infrastructure technology, consulting and applications, and product-related support services.

Customers trust Dell for their enterprise IT needs. They're the number one provider of Internet SCSI (iSCSI) storage solutions worldwide and the number one provider of x86 servers in the United States.

Dell Reconnect

Dell is committed to become the greenest technology company in the world as well as to advance the Green IT movement. Their plan is to become energy efficient and an environmental leader throughout their business. They have developed a global recovery and recycling supply chain on six continents to recycle the parts and materials they collect. Dell is also the first and only computer company offering free computer recycling to consumers worldwide.

Their business is aligned to address the unique needs of global corporations, small and medium businesses, government entities, healthcare providers, educational institutions and home computing users.

Corporate IT users recognize Dell as number one in customer satisfaction for services that include on-site expertise, on-site response time and phone support.

Forrester Research recognized Dell's initiatives to collect, interpret and react to feedback to improve customer experience with its Voice of the Customer Award.

Strategic Partnerships

CITRIX ORACLE BROCADE

intel redhat SanDisk

Microsoft SAP vmware

Industry Recognition

FORRESTER Gartner ESG Enterprise Strategy Group

Strategy & Implementation Plan

To increase City of Grand Junction's overall security posture, Sanity Solutions and Dell are positioning SonicWALL's SuperMassive Next Generation Firewall. Not all next-generation firewalls are the same. Dell SonicWALL NGFWs are capable of providing organizations of any size with a deeper level of network security because they are designed using a scalable, multi-core hardware architecture and a patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (see System Review) engine that scans all traffic regardless of port or protocol. Dell NGFWs ensure that every byte of every packet is inspected while maintaining the high performance and low latency that busy networks require.

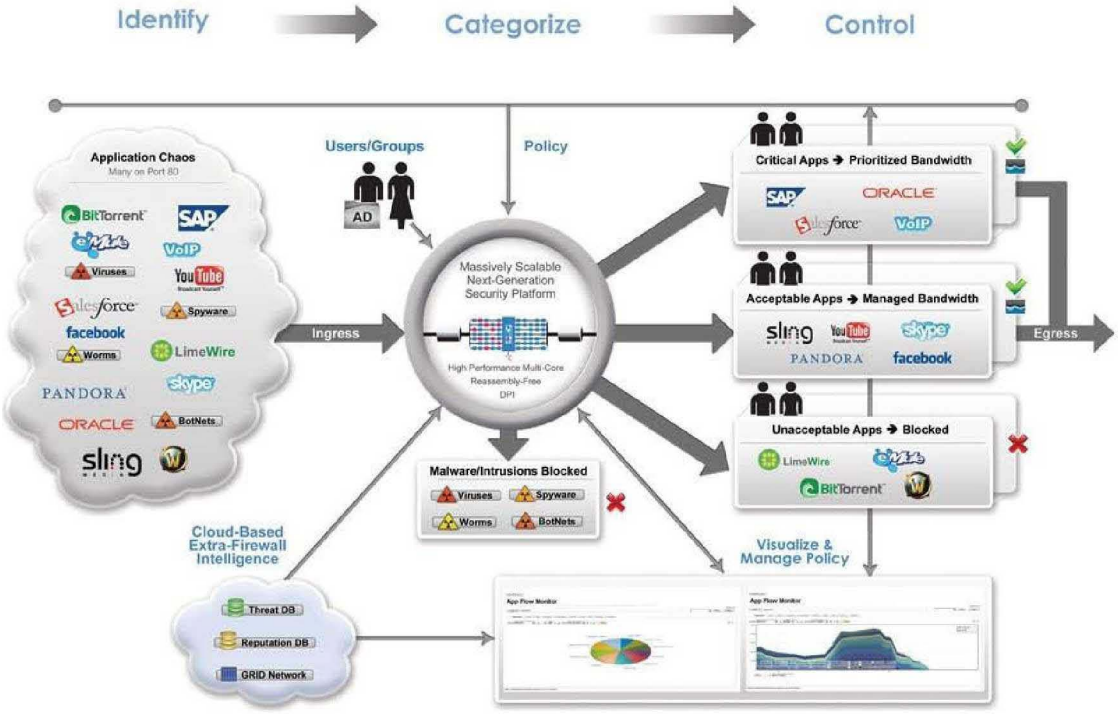
Additionally, in order to combat emerging threats effectively and address rising productivity concerns, organizations such as City of Grand Junction require a deeper level of security and control that includes an IPS with advanced anti-evasion capabilities, the ability to decrypt and inspect every SSL-encrypted connection crossing the network (on any port), granular control over and visibility into application and user activity across the network, and network-based malware protection that leverages the power of the cloud.

Dell SonicWALL has been recognized by industry analysts as leaders in firewalls and comprehensive security and protection. Gartner consistently recognizes SonicWALL as a leader in Unified Threat Management, or the combination of firewall/intrusion prevention system (IPS)/virtual private network, secure Web gateway security (URL filtering, Web antivirus) and messaging security (anti-spam, mail AV). (Reference Gartner Magic Quadrant)

NSS Labs, the world's leading information security research and advisory company, evaluates nine leading NGFW products every year for security effectiveness, performance, enterprise management capabilities against total cost of ownership- basically an assessment of how much bang for your buck. SonicWALL consistently ranks as a leader and 'recommended' in this annual report. (Reference NSS Labs Report)

Dell SonicWALL Next Generation Firewalls offer the ability for the administrator to create application policy to inspect encrypted (SSL) and non-encrypted traffic. Policies can be made to prevent access to cloud storage (ie. Google Drive, Dropbox, box.com, etc), webmail attachments (ie. Gmail, yahoo mail, hotmail, etc.), IM file transfers (Skype, gtalk, jabber, etc) and more. Dell leads the industry in overall threat management, due to the breadth of their portfolio and holistic approach to security posture.

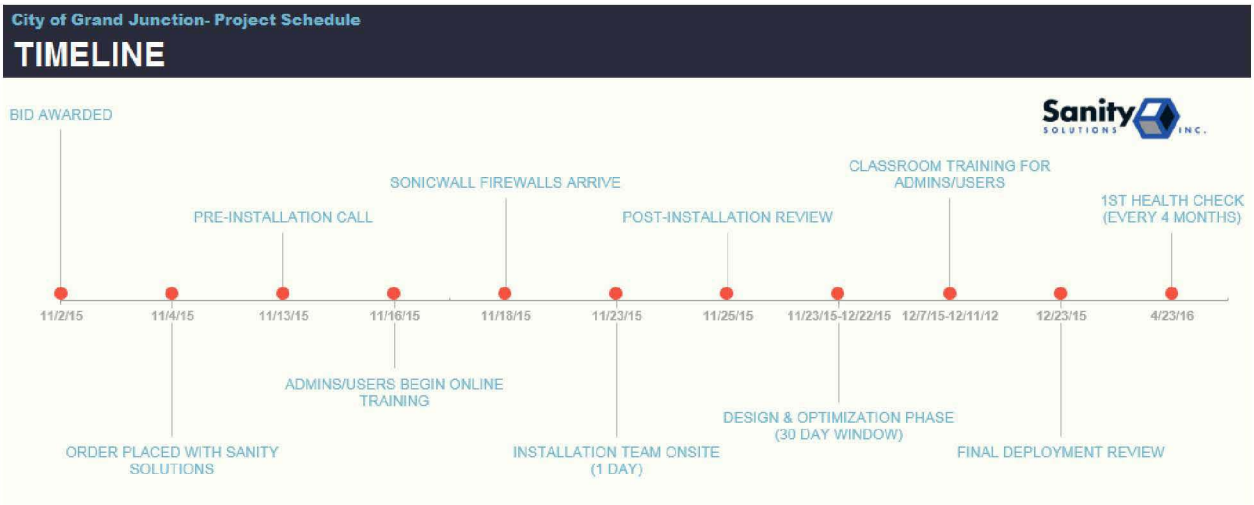
In addition to application policies, the Dell SonicWALL NGFW can provide intrusion prevention, botnet filtering, and malware protection, all of which can be sources of data loss. Dell SonicWALL also has email security devices that provides inbound and outbound filtering, compliancy filtering with expression matching, and encryption services. Alongside Dell's other security solutions and services- Disk & Endpoint Encryption, ID & Access Management, Security & Risk Consulting, and Managed Security Services- via the merge of technology, proper monitoring, and overall procedural diligence.



Installation, Optimization & Training

SonicWALL offers a very intuitive platform, however it is also very robust so training will be important to the primary users of the platform. Prior to the deployment of the firewall, we receommend admins/users take the free online prerequisite courses to prepare them for the new system. Then after deployment formal training will be provided to ensure advanced knowledge for all staff using the SonicWALL platform.

A senior field engineer will come onsite to install and deploy the system into the City's production environment. At this time all physical components will be completed and an initial knowledge transfer will be made between the engineer and the City staff who will be the primary users. Then technicians from Sanity and SonicWALL will work to cover all additional features including but not limited to AD integration, setting up rules and policies, application throttling and visibility, etc.. Detailed SOW will be prepared after pre-installation call. Sanity Solutions and Dell commit to the successful completion of this project, meeting or exceeding all expectations for the solution.



Specification Confirmation

4.3.1. The SM9200 firewall can be managed by both a web based GUI and CLI. Once familiarized with the platform, our customers find the GUI to be highly intuitive and exceptionally powerful.

4.3.2. Dell provides 24x7x365 support globally for their SonicWALL devices, with different SLA onsite options available. This solution includes Gold coverage, please see details of coverage in the Support Overview.

4.3.3. SonicWALL SSL/VPN authentication supports two-form authentication using hard and soft tokens via the RSA Authentication Manager. We would like to discuss this further to ensure any additional features or solutions should be considered her to match your specific requirement.

4.3.4. Dell SonicWALL NGFWs meet strict government compliance policies and are CJIS Compliant with FIPS-120 and Common Criteria. Please see details Government Review.

4.3.5. The VPN technology has both client and clientless functionality, supporting all required OS listed.

4.3.6. All data transmitted outside the boundary of a physically secure location is encrypted using certified 128-bit encryption. Review all encryption levels in the system specs.

4.3.7. The firewall will fail closed during a hardware or software failure.

4.3.8. The firewall can throttle network traffic based on a variety of traffic, discussed in the System Review

4.3.9. The firewall can support well beyond 500 internet users, outlined in the System Specs.

4.3.10. The firewall can perform detailed traffic analysis reporting via the Analyzer platform, detailed here.

4.3.11. All system logs are sent to centralized system within Analyzer, detailed here.

4.3.12. Real-Time alerts can be configured to notify admins based on a specific criteria.

4.3.13. The firewall supports up to 4x 10Gb and 8x 1Gb network interfaces, visit System Specs for more details.

4.3.14. Firewall can perform traditional port filtering.

4.3.15. Firewall supports both dynamic and static NAT and PAT.

4.3.16. Firewall fully supports all firewall features using IPv4 and IPv6, see System Specs.

4.3.17. The system has advanced application filtering, review Product Overview and Features.

4.3.18. Training included in solution, please see Cost Proposal.

4.3.19. The system has full integration with AD. This will be configured with Sanity and Dell PS teams.

4.3.20. The solution includes 25 SSL VPN licenses, please see Cost Proposal.

4.3.21. The solution includes a fully redundant HA unit with full functionality during failover, see cost proposal.

4.3.22. The solution includes extensive web content filtering for all internal users using AD to identify, track and report. For highly advanced filtering needs, especially for remote/mobile users, SonicWALL's Secure Mobile Access solution should be considered. See full review here, pricing available upon request.

4.3.23. Extensive reporting is available via Analyzer, full review here.

Support & Maintenance Details

This solution includes Gold Support, which provides the advanced support enterprises need to keep their networks running reliably and securely. Gold Support includes:

- Direct access. 24x7x365 access to a team of seasoned support engineers located at a Dell SonicWALL Enterprise TAC
- Around-the-clock support. 24x7x365 telephone, email and web-based technical support
- Software/firmware updates. For all software and firmware updates and upgrades
- Hardware replacement. Advanced exchange for replacement of defective hardware
- Support tools. Access to Dell SonicWALL's electronic support tools

Dell SonicWALL Comprehensive GMS Support Service delivers all the benefits of a Dynamic Support 24x7 contract for every eligible Dell SonicWALL appliance managed through a Dell SonicWALL GMS deployment. Comprehensive GMS also provides support and software updates for the GMS application. And, because you're purchasing a single co-terminus contract, there's only one expiration date for everything, simplifying management and administration while also removing the likelihood of lapsed support coverage.'

Regardless of your support contract, Dell SonicWALL provides a wealth of online technical information. It's a good idea to review this information prior to requesting support as you may find fast resolution to your issue.

- **Documentation**
  All of Dell SonicWALL's product documentation is available online in Adobe Acrobat format at http://www.sonicwall.com/us/support/2354.html.
- **Knowledge Portal**
  Dell SonicWALL's state-of-the-art Knowledge Base system is a simple-to-use system that provides answers to installation, configuration and troubleshooting questions. The Knowledge Base is updated daily with the most current information about our network security, secure remote access, content security, backup and recovery, and policy and management solutions.
- **The Forum**
  Our online, moderated Forum is a great place to get technical assistance, ideas and suggestions from the Dell SonicWALL user community. You'll find The Forum at https://forum.sonicwall.com/. Use your MySonicWALL.com account to log onto the Forum and post questions and answers to other Dell SonicWALL users, customers and employees.
- **Software and Firmware Updates**
  Software and firmware downloads are available on the Download Center at MySonicWALL.com. You will be presented with the list of updates you are entitled to when you select the "Type." Updates are limited to customers with valid service contracts.

Software & Firmware Updates

Customers can maintain software and firmware versions on its Dell SonicWALL Product(s), via download from the Dell SonicWALL Support web site (http://www.MySonicWALL.com), to levels consistent with the minimum supported versions. As standard policy, Dell SonicWALL's support

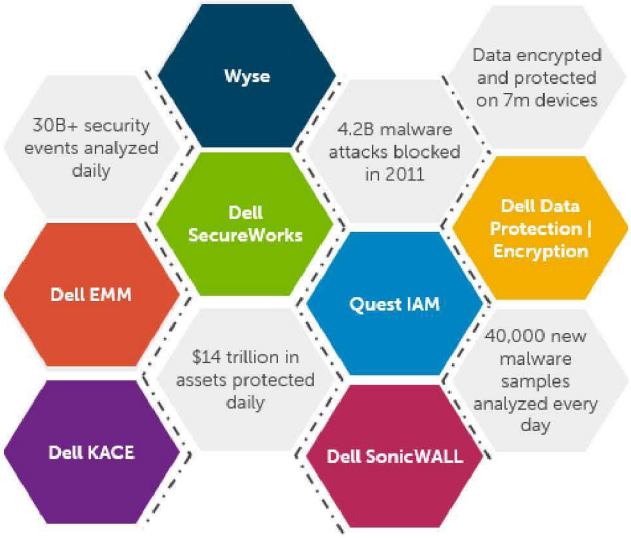
obligation extends only to the two most recent point releases of the then shipping software/firmware version, and the two most recent point releases of the major release immediately preceding such software/firmware version, inclusive of all drivers and firmware associated with these major/point release combinations.

Software and firmware downloads are available on the Download Center at MySonicWALL.com. You will be presented with the list of updates you are entitled to when you select the "Type." Updates are limited to customers with valid service contracts.

Major releases are signified by the integer preceding the first delimiter in the software/firmware version string, while the point release is indicated by the integer immediately following the first delimiter in the software/firmware version string (e.g. for the software/firmware version designated 3.04.02, the major release is 3, and the point release is 4).

Above and Beyond Scope of Project

While the solution designed in this proposal is robust and meets or exceeds City of Grand Junction's requirements for this project, Sanity and Dell have a wide portfolio of integrated security solutions and strategic partnerships with the unique ability to enhance end-to-end protection of data within the organization. These include Identity & Access Management, Endpoint Encryption, Asset & Mobile Device Management, and Managed Security Services. We would encourage a full security assessment (which could include Penetration Testing, Control Audits, Information Security Assessment, etc.) to identify vulnerabilities and dramatically improve overall security posture across the organization.



References

Powdr Corp
PO BOX 980430
Park City, Utah 84098
Craig Casey
435-658-5820
CCasey@powdr.com

Woodford Manufacturing
2121 Waynoka Rd.
Colorado Springs, CO 80915
Paul Talbert
(800) 621-6032
ptalbert@wcmind.com

ShopAtHome.com
5575 DTC Parkway #300
Greenwood Village, CO 80111
Jon Seashore
(303) 625-6994
jseashore@belcarogroup.com

Sanity Solutions & Dell Partnered Colorado Based Government Customers

Cherry Creek Schools
Adams County
City of Aurora
Mesa County
Platte River Power Authority
Department of Energy- NOAA, NREL, LM
Department of Commerce- Census, ONRR
Department of Interior- BOR, NPS

Dell SonicWALL Reference Customers
(Click link for more information)

Denver Broncos Organization
Walton County Public Schools
Weber County
Cedarville University
Amerijet Holdings

Fee Proposal

Keith Barnholt
Email: kbarnholt@sanitysolutions.com
Phone: 720.570.1668 x614
Fax: 866.826.5681

Date: September 30, 2015
Quote Expires: 30 day(s)

Quotation # 005023-R0

Contact:
City of Grand Junction
250 North 5th Street
Grand Junction, CO 81501-2668

NEXT GENERATION FIREWALL

PRODUCT	DESCRIPTION	QTY	UNIT PRICE	TOTAL
UUFW-01-SSC-3816	**Dell SonicWALL SuperMassive 9200 Next Generation Firewall** Comprehensive Gateway Security Suite Includes: -Intrusion Prevention -Gateway Anti-Virus -Anti-Spyware -Application Control & Visualization -Cloud AV -Content Filtering Premium Service -Botnet filtering -GeoIP Identification 2 Years 24x7 Gold Support & Maintenance Includes: 6x 10GB SFP+ COPPER WITH 3M TWINAX CABLE 3x 10GB SFP+ COPPER WITH 1M TWINAX CABLE	1	$44,800.00	$44,800.00
UUFW-01-SSC-3811	**Dell SonicWALL SuperMassive 9200 High Availability Appliance** 2nd Unit- Both Appliances Configured Equally	1	$18,897.00	$18,897.00
UUFW00-A7487614	**Dell SonicWALL SLL VPN- 25 Users**	1	$350.00	$350.00
UUSW00-A7483569	**Dell SonicWALL Analyzer**	1	$950.00	$950.00

TRAINING

PRODUCT	DESCRIPTION	QTY	UNIT PRICE	TOTAL
UUSV-01-SSC-8500	**1 Week Comprehensive SonicWALL Instructor Led Admin Training- 1 Seat** Network Security Basic Administrator Training with Test Out Secure Mobile Access Basic Administrator Training with Test Out	3	$4,790.00	$14,370.00

Sanity SOLUTIONS INC.

PROFESSIONAL SERVICES

PRODUCT	DESCRIPTION	QTY	UNIT PRICE	TOTAL
SSSV-GTCNTRCTINSTALL	**Professional Services** Estimated Deployment & Optimization Services	1	$8,750.00	$8,750.00
			SUBTOTAL	**$8,750.00**

Leasing option available upon request.

Comments: **Sanity Solutions & Dell Customer Loyalty Discount Applied**

Subtotal:	$88,117.00
Discount:	($23,450.00)
Total:	**$64,667.00**

Thank you for giving Sanity Solutions the opportunity to earn your business. If you have not yet received our Terms & Conditions, please ask your Account Executive.

Shipping and tax not included unless indicated.

Net 30

Solicitation Response Form

Warranty

DELL Software

Support and Professional Services

Survival of the fittest still applies

We don't mean to be alarmists, but your network is under siege. There are thousands of well-known threats to your network already in existence, and new ones are launched every day. To keep your network safe, your security and data protection solutions have to be every bit as dynamic as the threats they're guarding against.

That's where Dell™ SonicWALL™ network security and data protection solutions and ongoing services come in. With them, your network will be protected against the ever-changing world of cyber crime. And our wide range of services can be tailored to suit your unique needs, helping you prepare, manage and update your network security infrastructure.

The range of services includes:

- Dell SonicWALL Dynamic, Silver, E-Class and Gold Support Services
- Dell SonicWALL Premium Support Services
- Dell SonicWALL Professional Services

Dell SonicWALL Global Support Services

Dell SonicWALL designed its support services not only to keep your network security and data backup and recovery infrastructure current, but to also react swiftly to any problem that may occur. However that's not enough to keep your network safe these days. So, Dell SonicWALL's support services also include crucial software and firmware updates and upgrades, the finest technical support, timely hardware replacement and access to extensive electronic tools.

Dynamic Support
Designed for customers who need continued protection through on-going firmware updates and advanced technical support, Dell SonicWALL Dynamic Support is available during normal business hours, or 24x7, depending on your needs. Services include:

- Subscription to firmware updates and upgrades
- Access to chat, email, web and telephone support
- Advance Exchange hardware replacement in the event of failure

Silver Support
More than a traditional break-fix service, Dell SonicWALL Silver Support is a multi-layered security offering that provides you with access to critical firmware updates and upgrades plus expert technical assistance to keep your Dell SonicWALL solution performing optimally. Services include:

- Subscription to firmware updates and upgrades
- 8x5 or 24x7 access to chat, email, web and telephone technical support
- Advance Exchange Next Business Day hardware replacement in the event of failure

E-Class Support
Available only on E-Class products, E-Class Support provides the enterprise-class support features and quality of service companies require to keep their networks running smoothly and efficiently. E-Class Support includes all the features of our Dynamic Support offerings PLUS 24x7 direct access to a team of highly-trained senior support engineers located at a Dell SonicWALL Enterprise TAC.

Gold Support
Exclusive to NSA 5600, NSA 6600 and SuperMassive 9000 Series Next-Generation Firewalls, Gold Support provides the advanced support features enterprise organizations need to keep their networks running reliably and securely. With Gold Support, you have around-the-clock access to seasoned support engineers at a Dell SonicWALL Enterprise TAC and the latest firmware features plus Advance Exchange hardware replacement, all of which combine to protect and maximize your Dell SonicWALL investment.

Comprehensive Global Management System (GMS)
For customers using Dell SonicWALL Global Management System (GMS) to manage their distributed networks, there's Dell SonicWALL Comprehensive GMS. This umbrella support service delivers all the benefits of a Dynamic Support 24x7 contract for every Dell SonicWALL appliance managed through a Dell SonicWALL GMS deployment. Not only that, Comprehensive GMS provides support and software updates for the GMS application itself. And, because you're purchasing a single co-terminus contract, there's only one expiration date for Dell SonicWALL support contracts on all eligible appliances, simplifying management and administration while also removing the likelihood of lapsed support coverage.

Warranty support
All Dell SonicWALL appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty.

Service offering	Hours of availability	Chat support[2]	Phone, email and web support	Firmware updates	Hardware warranty	RMA fulfillment	Technical Assistance Center (TAC)
Gold support	24x7	●	●	●	1 Year[1]	Advance Exchange[4]	Enterprise TAC
E-Class support	24x7	●	●	●	1 Year[1]	Advance Exchange[4]	Enterprise TAC
Silver support	8x5[3] or 24x7	●	●	●	1 Year[1]	Advance Exchange[4]	SMB or Advanced TAC[5]
Dynamic support	8x5[3] or 24x7	●	●	●	1 Year[1]	Advance Exchange[4]	SMB or Advanced TAC[5]
Comprehensive GMS	24x7	●	●	●	1 Year[1]	Advance Exchange[4]	SMB, Advanced or Enterprise TAC[5]

Dell SonicWALL Professional Services

Dell SonicWALL offers a range of Professional Services to meet your needs, from our Remote Start-up and Configuration Service to our traditional statement of work-based services. Combined with their detailed knowledge of Dell SonicWALL products and services, Dell SonicWALL consultants bring wide industry experience, tested methodologies, and the backing of Dell SonicWALL's world-class engineering support to every engagement. With Dell SonicWALL Professional Services, you get some of the brightest people in the industry working for you.

Dell SonicWALL Remote Start-up and Configuration Service

Dell SonicWALL Remote Start-up and Configuration Service provides secure remote configuration of your Dell SonicWALL TZ or Email Security appliance. A Certified Dell SonicWALL Security Administrator (CSSA) - Dell SonicWALL engineer works with you via email and over the phone to build a configuration plan based on your requirements. Once you've agreed to the plan, the Dell SonicWALL security engineer will configure your appliance quickly and efficiently for rapid deployment into your network. Whether it's one appliance or 100, Remote Start-up and Configuration Service can help you minimize your costs by taking care of one of the most important aspects of your deployment plan so that you can focus on the others.

- Dell SonicWALL Remote Start-up and Configuration Service for the TZ Series
- Dell SonicWALL Remote Start-up and Configuration Service for Email Security Appliances

Dell SonicWALL Jump Start

Time is money, so getting a jump on deploying technologies that speed your product or service to market is imperative. For the fastest and most optimal deployment of your Dell SonicWALL E-Class appliance, on-site expert assistance is essential. Dell SonicWALL Jump Start makes deployment of your next-generation security solution easy and seamless with expert guidance and deployment planning assistance. An experienced Dell SonicWALL Systems Engineer (SE) will review your implementation plans, security configurations and project goals to formulate a best practices approach to meet your requirements.

- Dell SonicWALL Jump Start for the E-Class Network Security Appliance Series
- Dell SonicWALL Jump Start for the E-Class Secure Remote Access Series

Custom consulting services

Enterprise networks have a whole set of unique security and data protection needs. Dell SonicWALL Custom Consulting Services provide customized, project-based consulting to meet these demands. These services include:

- Security Assessments—Dell SonicWALL examines your network, determines the security level and exposes any potential holes in firewalls, routers and other network devices. We then compile comprehensive reports that examine your internal network, analyze how it appears to perpetrators and give detailed corrective actions.
- Security Design and Implementation—for customers who need a comprehensive approach to network security, Dell SonicWALL evaluates overall security and then designs and implements the appropriate solutions. This includes security policy development to ensure the security solution is built on a solid foundation.

Additional Data

Product Overview

Dell SonicWALL SuperMassive Series

Network security

The Dell™ SonicWALL™ SuperMassive™ Series is Dell's next-generation firewall (NGFW) platform designed for large networks to deliver scalability, reliability and deep security at multi-gigabit speeds with near zero latency.

Built to meet the needs of enterprise, government, university, and service provider deployments, the SuperMassive Series is ideal for securing enterprise networks, data centers and service providers.

Combining its massively multi-core architecture and Dell SonicWALL's patented* Reassembly-Free Deep Packet Inspection® (RFDPI) technology, the SuperMassive E10000 and 9000 Series deliver industry-leading application control, intrusion prevention, malware protection and SSL inspection at multi-gigabit speeds. The SuperMassive Series is designed with power, space, and cooling (PSC) in mind, providing the leading Gbps/Watt NGFW in the industry for application control and threat prevention.

The Dell SonicWALL RFDPI engine scans every byte of every packet across all ports, delivering full content inspection of the entire stream while providing high performance and low latency. This technology is superior to outdated proxy designs that reassemble content using sockets bolted to anti-malware programs that are plagued with inefficiencies and overhead of socket memory thrashing that leads to high latency, low performance and file size limitations. The RFDPI engine delivers full content inspection to eliminate threats before they enter the network and provides protection against millions of unique malware variants without file size, performance or latency limitations. The RFDPI engine also provides full inspection of SSL-encrypted traffic as well as non-proxyable applications enabling complete protection regardless of transport or protocol.

Application traffic analytics allow for the identification of productive and unproductive application traffic in real time which can then be controlled through powerful application-level policies. Application control can be exercised on both a per-user and per-group basis, along with schedules and exception lists. All application, intrusion prevention, and malware signatures are constantly updated by the Dell SonicWALL Threats Research Team. Additionally, SonicOS, an advanced purpose-built operating system, provides integrated tools that allow for custom application identification and control.

The design of the SuperMassive Series firewalls provides near-linear performance and scales up to 96 cores of processing power to deliver up to 40 Gbps of firewall throughput, 30 Gbps of threat prevention and 30 Gbps of application inspection and control. The SuperMassive E10000 Series is field upgradeable, future-proofing the security infrastructure investment as network bandwidth and security requirements increase.

U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

SuperMassive E10000 Series

SuperMassive 9000 Series

Benefits:

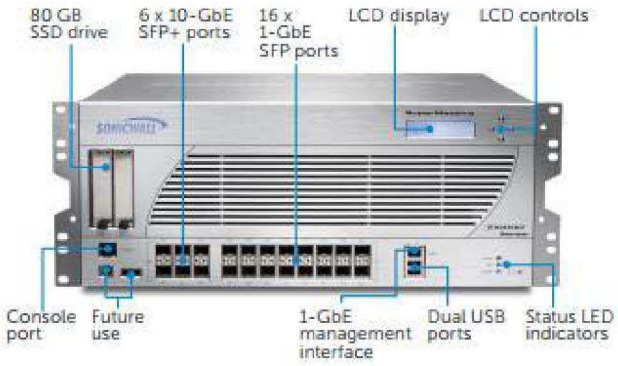
- Complete threat protection including high performance intrusion prevention and low latency malware protection
- Superior granular application intelligence, control and visualization
- Full inspection of SSL encrypted traffic without overhead, latency, and memory thrashing associated with socket-based SSL proxies
- Massively scalable multicore architecture designed for 10/40 Gbps infrastructure

Series lineup

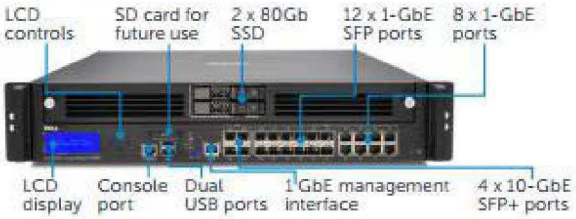
The Dell SonicWALL SuperMassive E10000 Series chassis includes 6 x 10-GbE SFP+ and 16 x 1-GbE SFP ports, redundant 850W AC power supplies, hot swappable dual redundant fan modules, and massively scales up to 96 processing cores.

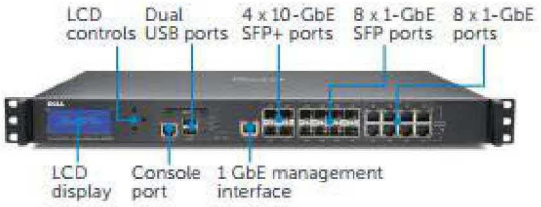
The Dell SonicWALL SuperMassive 9000 Series features 4 x 10-GbE SFP+, up to 12 x 1-GbE SFP, 8 x 1-GbE Copper and 1 GbE management interfaces, with an expansion port for an additional 2 x 10-GbE SFP+ interfaces (future release). The 9000 Series features hot swappable fan modules and power supplies.

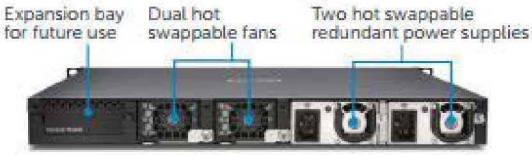
SuperMassive E10000 Series



SuperMassive 9000 Series



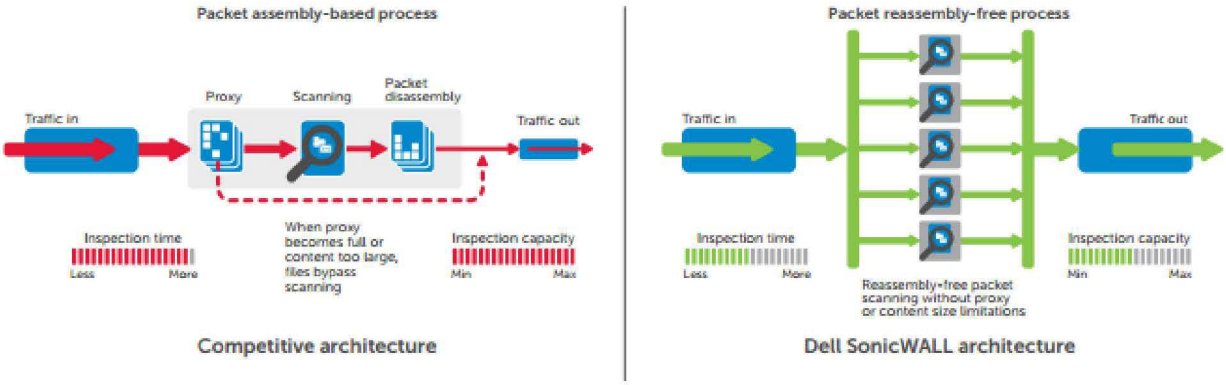




Capability	9200	9400	9600	9800	E10400	E10800
Processing cores	24	32	32	64	48	96
Firewall throughput	15 Gbps	20 Gbps	20 Gbps	40 Gbps	20 Gbps	40 Gbps
Application intelligence throughput	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps	15 Gbps	28 Gbps
IPS throughput	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps	15 Gbps	28 Gbps
Anti-malware	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps	6 Gbps	12 Gbps
Maximum DPI Connections	1.25 M	1.25 M	1.5 M	2.5 M	5 M	10 M
Deployment Modes	**9200**	**9400**	**9600**	**9800**	**E10400**	**E10800**
L2 Bridge, Transparent Mode	Yes	Yes	Yes	Yes	Yes	Yes
Wire Mode	Yes	Yes	Yes	Yes	Yes	Yes
Gateway/NAT Mode	Yes	Yes	Yes	Yes	Yes	Yes
Tap Mode	Yes	Yes	Yes	Yes	Yes	Yes
Transparent Bridge Mode	Yes	Yes	Yes	Yes	Yes	Yes

Reassembly-Free Deep Packet Inspection engine

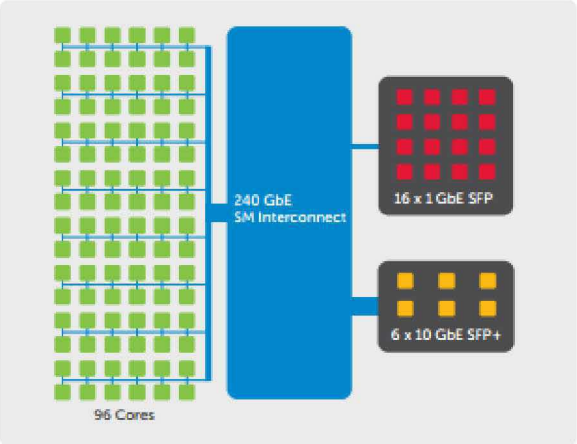
The RFDPI engine provides superior threat protection and application control without compromising performance. This patented engine relies on streaming traffic payload inspection in order to detect threats at Layers 3-7. The RFDPI engine takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network. Once a packet undergoes the necessary pre-processing, including SSL decryption, it is analyzed against a single proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken. In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified.



Extensible architecture for extreme scalability and performance

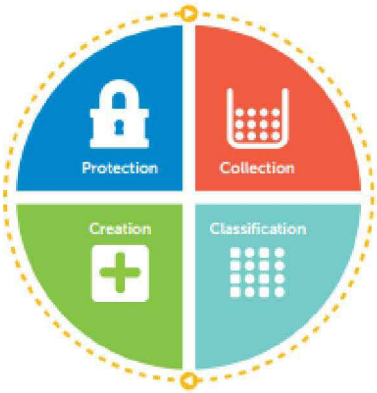
The RFDPI engine is designed from the ground up with an emphasis on providing security scanning at a high level of performance, to match both the inherently parallel and ever-growing nature of network traffic. When combined with 24-, 32-, 48-, 64- or 96-core processor systems, this parallelism-centric software architecture scales up perfectly to address the demands of deep packet inspection at high traffic loads. The SuperMassive platform relies on processors that, unlike x86, are optimized for packet, crypto and network processing while retaining flexibility and programmability in the field—a weak point for ASICs systems. This flexibility is essential when new code and behavior updates are necessary to protect against new attacks that require updated and more sophisticated detection techniques.

Another aspect of the platform design is the unique ability to establish new connections on any core in the system, providing ultimate scalability and the ability to deal with traffic spikes. This approach delivers extremely high new session establishment rates (new conn/sec) while deep packet inspection is enabled—a key metric that is often a bottleneck for data center deployments.



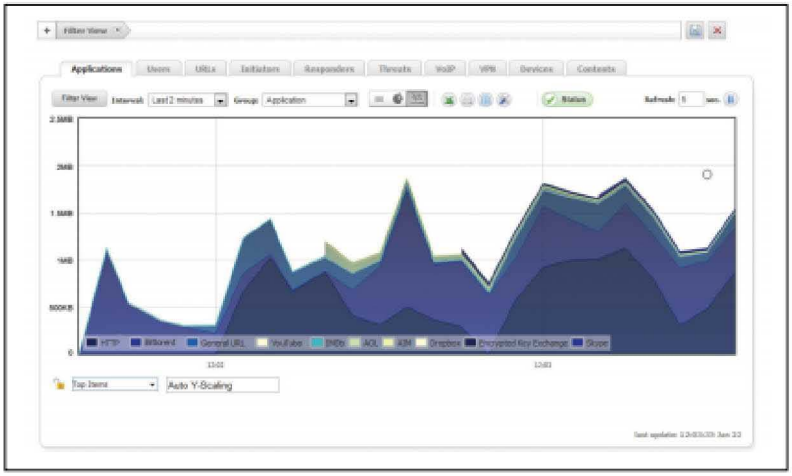
Security and protection

The dedicated, in-house Dell SonicWALL Threats Research Team works on researching and developing countermeasures to deploy to the firewalls in the field for up-to-date protection. The team leverages more than one million sensors across the globe for malware samples, and for telemetry feedback on the latest threat information, which in turn is fed into the intrusion prevention, anti-malware and application detection capabilities. Dell SonicWALL NGFW customers with the latest security capabilities are provided continuously updated threat protection around the clock, with new updates taking effect immediately without reboots or interruptions. The signatures on the appliances protect against wide classes of attacks, covering up to tens of thousands of individual threats with a single signature. In addition to the countermeasures on the appliance, SuperMassive firewalls also have access to the Dell SonicWALL CloudAV Service, which extends the onboard signature intelligence with more than seventeen million signatures, and growing. This CloudAV database is accessed via a proprietary light-weight protocol by the firewall to augment the inspection done on the appliance. With Geo-IP and botnet filtering capabilities, Dell SonicWALL NGFWs are able to block traffic from dangerous domains or entire geographies in order to reduce the risk profile of the network.



Application intelligence and control

Application intelligence informs administrators of application traffic traversing their network, so they can schedule application controls based on business priority, throttle unproductive applications, and block potentially dangerous applications. Real-time visualization identifies traffic anomalies as they happen, enabling immediate countermeasures against potential inbound or outbound attacks or performance bottlenecks.



Dell SonicWALL Application Traffic Analytics provide granular insight into application traffic, bandwidth utilization and security threats, as well as powerful troubleshooting and forensics capabilities. Additionally, secure single sign-on (SSO) capabilities ease user experience, increase productivity and reduce support calls. Management of application intelligence and control is simplified by using an intuitive web-based interface.

Global Management and Reporting

For larger, distributed enterprise deployments, the optional Dell SonicWALL Global Management System (GMS®) provides administrators a unified, secure and extensible platform to manage Dell SonicWALL security appliances. It enables enterprises to easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities and governs all operational aspects of the security infrastructure including centralized policy management and enforcement, real-time event monitoring, analytics and reporting, and more. GMS also meets the firewall change management requirements of enterprises through a workflow automation feature. With GMS workflow automation, all enterprises will gain agility and confidence in deploying the right firewall policies, at the right time, and in conformance to compliance regulations. GMS provides a better way to manage network security by business processes and service levels that dramatically simplify the lifecycle management of your overall security environments rather than on a device-by-device basis.

Features

RFDPI engine	
Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts, malware and identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware, and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and for application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

Intrusion prevention	
Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The Dell SonicWALL Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly detection and prevention	Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

Features

Threat prevention	
Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
CloudAV	A continuously updated database of over 17 million threat signatures resides in the Dell SonicWALL cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with an extensive coverage of threats.
Around-the-clock security updates	The Dell SonicWALL Threat Research Team analyzes new threats and releases countermeasures 24 hours a day, 7 days a week. New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
SSL inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in SSL encrypted traffic.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally, preventing attacks that try to sneak by outdated security systems that focus on securing a few well-known ports.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMB v1/v2 and others, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard well known ports.

Application intelligence and control	
Feature	Description
Application control	Controls applications, or individual application features, which are identified by the RFDPI engine against a continuously expanding database of over 3600 application signatures, to increase network security and enhance network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.
Application bandwidth management	Granularly allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic.
On-box/off-box traffic visualization	Identifies bandwidth utilization and analyzes network behavior with real-time on-box application traffic visualization and off-box application traffic reporting via NetFlow/IPFix.
Granular control	Controls applications, or specific components of an application, based on schedules, users groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/ Terminal Services/Citrix integration.

Features

Content Filtering	
Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to websites containing information or images that are objectionable or unproductive with Content Filtering Service. Extend policy enforcement to block internet content for devices located outside the firewall perimeter with the Content Filtering Client.
Granular controls	Block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Dynamic rating architecture	All requested web sites are cross-referenced against a dynamically updated database in the cloud categorizing millions of URLs, IP addresses and domains in real time.
YouTube for Schools	Enable teachers to choose from hundreds of thousands of free educational videos from YouTube EDU that are organized by subject and grade and align with common educational standards.
Web caching	URL ratings are cached locally on the Dell SonicWALL firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.

Enforced anti-virus and anti-spyware	
Feature	Description
Multi-layered protection	A firewall's gateway anti-virus solution provides the first layer of defense at the perimeter, however viruses can still enter the network through laptops, thumb drives and other unprotected systems. Utilize a layered approach to anti-virus and anti-spyware protection to extend to both client and server.
Automated enforcement	Ensure every computer accessing the network has the most recent version of anti-virus and anti-spyware signatures installed and active, eliminating the costs commonly associated with desktop anti-virus and anti-spyware management.
Automated deployment and installation	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Always on, automatic virus protection	Frequent anti-virus and anti-spyware updates are delivered transparently to all desktops and file servers to improve end user productivity and decrease security management.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.

Features

Firewall and networking	
Feature	Description
Stateful Packet Inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DDoS/DoS attack protection	SYN Flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it provides the ability to protect against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The SuperMassive Series can be deployed in traditional NAT, Layer 2 Bridge, Wire Mode, and Network Tap modes.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With the latest SonicOS 6.2, the hardware will support Filtering and wire mode implementations.
High availability/clustering	The SuperMassive Series supports Active/Passive with state synchronization, Active/Active DPI and Active/Active Clustering high availability modes. Active/Active DPI offloads the Deep Packet Inspection load to cores on the passive appliance to boost throughput.
WAN load balancing	Load balances multiple WAN interfaces using Round Robin, Spillover or Percentage based methods.
Policy-based routing	Creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.
Advanced QoS	Guarantees critical communications with 802.1p and DSCP tagging, and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.

Management and reporting	
Feature	Description
Global Management System	With Dell SonicWALL GMS, monitors, configures and reports on multiple Dell SonicWALL appliances through a single management console with an intuitive interface, to reduce management costs and complexity.
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive CLI and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools, such as Dell SonicWALL Scrutinizer or other tools that support IPFIX and NetFlow with extensions.

Virtual Private Networking	
Feature	Description
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the SuperMassive Series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless automatic failover and failback of all VPN sessions.

Features

Virtual Private Networking (continued)	
Feature	Description
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.

Content/context awareness	
Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix[1]/Terminal Services[1] SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network.
Regular Expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

SonicOS feature summary

Firewall
- Reassembly-Free Deep Packet Inspection
- SSL decryption and inspection
- Stateful packet inspection
- Stealth mode
- Common Access Card (CAC) support
- DOS attack protection
- UDP/ICMP/SYN Flood Protection
- IPv6 Security
- Management and monitoring: IPv4 and IPv6 Management
- Networking: IPv6

Intrusion prevention
- Signature-based scanning
- Automatic signature updates
- Bidirectional inspection engine
- Granular IPS rule set
- GeoIP and Reputation-based filtering
- Regular Expression matching
- UDP/ICMP/SYN Flood protection

Anti-Malware
- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application intelligence
- Application control
- Application component blocking
- Application bandwidth management
- Custom application signature creation
- Application Traffic Visualization
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- User activity tracking (SSO)
- Comprehensive application signature database

Web content filtering
- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- 56 Content filtering categories
- Content Filtering Client (SonicOS 6.2)

VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSEC client remote access
- Redundant VPN gateway
- Mobile Connect for Apple® iOS and Google® Android™
- Route-based VPN (OSPF, RIP)

Networking
- Jumbo Frames (SonicOS 6.0.5 and 6.2 only)
- Path MTU Discovery
- Enhanced Logging
- VLAN Trunking
- Layer-2 Network Discovery
- Port Mirroring
- Layer-2 QoS
- Port Security
- Dynamic routing
- SonicPoint wireless controller[1]
- Policy-based routing
- Advanced NAT
- DHCP server
- Bandwidth Management
- Link aggregation
- Port redundancy
- A/P High availability with State Sync
- A/A Clustering
- Inbound/Outbound Load balancing
- L2 Bridge, Wire mode, Tap Mode, NAT Mode

VoIP
- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

Management and monitoring
- Web GUI
- Command line interface (CLI)
- SNMPv2/v3
- Off-Box reporting (Scrutinizer)
- Centralized management and reporting Global Management System policy management and reporting
- Logging
- Netflow/IPFix Exporting
- Application and bandwidth visualizer
- LCD management screen
- Centralized policy management
- Single Sign-On (SSO)
- Terminal service/Citrix support[1]
- BlueCoat Security Analytics Platform

[1] Supported on SonicOS 6.1 and 6.2. Not supported on SonicOS 6.2.1.

SuperMassive 9000 Series system specifications

	9200	9400	9600	9800
Operating system	SonicOS			
Security Processing Cores	24	32		64
10 GbE interfaces	4 x 10-GbE SFP+			
1 GbE interfaces	8 x 1-GbE SFP, 8 x 1 GbE (1 LAN Bypass pair)			12 x 1-GbE SFP, 8 x 1 GbE
Management interfaces	1 GbE, 1 Console			
Memory (RAM)	8 GB	16 GB	32 GB	64 GB
Storage	Flash			2x 80GB SSD, Flash
Expansion	1 Expansion Slot (Rear)*, SD Card*			
Firewall inspection throughput[1]	15 Gbps	20 Gbps		40 Gbps
Application inspection throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
IPS throughput[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
Anti-malware inspection throughput[2]	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps
IMIX performance	4.4 Gbps	5.5 Gbps		9 Gbps
SSL-DPI	1 Gbps	2 Gbps	2 Gbps	5 Gbps
VPN throughput[3]	5 Gbps	10 Gbps	11.5 Gbps	18 Gbps
Latency	17µs			
Connections per second	100,000/sec	130,000/sec		280,000/sec
Maximum connections (SPI)	1.25 M		1.5 M	3 M
Maximum connections (DPI)	1 M		1.25 M	2.5 M
SSO User	80,000	90,000	100,000	**110,000**
SonicPoints Supported (max)	128			-
VPN	**9200**	**9400**	**9600**	**9800**
Site-to-site tunnels	10,000			25,000
IPSec VPN clients (max)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)	2,000 (10,000)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF			
Networking	**9200**	**9400**	**9600**	**9800**
IP address assignment	Static, DHCP, PPPoE, L2TP and PPTP client, Internal DHCP server, DHCP Relay[4], Internal DHCP server, DHCP Relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT, transparent mode			
VLAN interfaces	512			
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, terminal services[5], Citrix[5]			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications	ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, CSfC, USGv6			
Certifications pending	FIPS 140-2, Common Criteria NDPP, ICSA Anti-Virus, UC-APL			
Hardware	**9200**	**9400**	**9600**	**9800**
Power supply	Dual, redundant, hot swappable, 300 W			Dual, redundant, hot swappable, 500 W
Fans	Dual, redundant, hot swappable			
Display	Front LED display			
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	200			350
MTBF @25ºC in Hours	188,719	187,702	186,451	126,144
MTBF @25ºC in Years	21.543	21.427	21.284	14.400
Form factor	1U Rack Mountable			2U Rack Mountable
Dimensions	17x19.1x1.75 in (43.3x48.5x4.5 cm)			17x24x3.5 in (9x60x43 cm)
Weight	18.1 lb (8.2 kg)			40.5 lb (18.38 kg)
WEEE weight	23 lb (10.4 kg)			49.5 lb (22.4 kg)
Shipping weight	29.3 lb (13.3 kg)			65 lb (29.64 kg)
Major regulatory	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TUVGS, CB, NOM, RoHS, WEEE , ANATEL, BSMI			
Environment	32-105 F, 0-40 deg C			15-40 deg C
Humidity	10-90% non-condensing			

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. [2] Full DPI/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.
[3] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change. *Future use. All specifications, features and availability are subject to change. [4] PPPoE, L2TP and PPTP clients are not supported on SM9800. [5] Supported on SonicOS 6.1 and 6.2

Analyzer

Application traffic analytics, visualization and reporting tool

When employees use web applications such as web mail, Facebook, instant messaging and BitTorrent for non-work-related activity, bandwidth utilization spikes, productivity plummets and threats to the network begin to emerge. IT needs a solution to strengthen security awareness, optimize network utilization, intelligently manage applications and cost effectively provide troubleshooting and forensics analysis. Most third-party application traffic analytics and reporting products do not achieve these objectives because they do not provide full network visibility and they can be complex to use.

By contrast, Dell™ SonicWALL™ Analyzer does meet these objectives. Analyzer is a web-based traffic analytics and reporting tool that is easy to use and provides real-time and historical insight into network health, performance and security. Analyzer supports Dell SonicWALL firewalls, backup and recovery products and secure remote access solutions. Organizations of all sizes benefit from enhanced employee productivity, optimized network bandwidth utilization and increased security awareness. Dell SonicWALL is the *only* firewall vendor that provides a complete solution by combining off-box application traffic analytics with granular data generated by Dell SonicWALL firewalls.

Benefits:

- Comprehensive graphical reports enable visibility and analysis of threats and activities
- Next-generation syslog reporting streamlines data summarization
- Powerful insights into Secure Remote Access and Continuous Data Protection appliance health and behavior
- Universal scheduled reports speed in-depth reporting
- At-a-glance reporting facilitates quick analysis
- Compliance reporting makes report generation easy
- Multi-threat reporting provides instant information on threats and attacks
- User-based reporting tracks activity across the entire network
- Ubiquitous access simplifies reporting for any location
- New attack intelligence enables granular reporting on specific attacks

Features

Comprehensive graphical reports — Provide visibility into firewall threats, bandwidth usage, employee productivity, suspicious network activity and application traffic analysis.

Next-generation syslog reporting — Revolutionary architecture streamlines data summarization, allowing for near real-time reporting of incoming syslog messages. Direct access to the underlying raw data further facilitates extensive granular capabilities and highly customizable reporting.

Dell SonicWALL Secure Remote Access and Continuous Data Protection reporting — Leverages next-generation syslog data to provide powerful insight into appliance health and behavior.

Universal scheduled reports — Provide a single entry point for all scheduled reports. One report can combine charts and tables for multiple units. Reports can be scheduled and sent out in various formats to one or more email addresses.

At-a-glance reporting — Offers customizable views to illustrate multiple summary reports on a single page. Users can easily navigate through vital network metrics to analyze data quickly across a variety of reports.

Compliance reporting — Enables administrators to generate reports that fulfill compliance requirements on an ad-hoc and scheduled basis for specific regulatory mandates.

Multi-threat reporting — Collects information on thwarted attacks, providing instant access to threat activities detected by Dell SonicWALL firewalls using the Dell SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service.

User-based reporting — Tracks individual user activities locally or on remote network sites. Provides greater insight into traffic usage across the entire network and, more specifically, application usage, websites visited, backup activity and VPN connections per user.

Ubiquitous access — Simplifies reporting to provide administrators with analysis of any location using only a standard web browser.

New attack intelligence — Offers granular reporting on specific types of attacks, intrusion attempts and the source address of the attack to enable administrators to react quickly to incoming threats.