



Town of Yacolt

202 W. Cushman Street - P.O. Box 160
Yacolt, WA 98675

Tel: (360) 686-3922 Fax: (360) 686-3853
townofyacolt.com

July 2nd, 2018

Town Council Agenda

Town Hall 7:00 p.m.

- 1. Call to Order**
- 2. Flag Salute**
- 3. Roll Call**
- 4. Minutes from the Previous Meeting**
 - A. Meeting Minutes for the June 18, 2018 Meeting**
- 5. Late Changes to the Agenda**
- 6. Citizen Communication**

***Anyone requesting to speak to the Council regarding items not on the Agenda may come forward at this time. Comments are limited to 3 minutes.**
- 7. Old Business:**
 - A. Council Action – Tabled Amboy Ave. Short Plat Application**
- 8. New Business:**
 - A. Laura Ellsworth – Council for the Homeless**
 - B. Donald Greenwalt – Setback Variance for Shed**
 - C. Contract with Michael Monen**
 - D. Rotate Mayor Pro-Tem**
 - E. Rotate Finance Committee**
- A. Mayor's Comments**
- B. Attorney's Comments**
- C. Council Comments**
- D. Public Works Dept. Report**

Summer temp help
- E. Town Clerks Report**

Computer analysis update-CCSI Quote-Dependable Computer Quote
Update on Advanced payroll upgrade
Treasurers reports for April and May
- F. Pay Bills on behalf of the Town**
- G. Adjourn**

The Town of Yacolt is celebrating 110 Years.... 1908 - 2018!

Town of Yacolt
202 W. Cushman St.
Yacolt, WA 98675

DRAFT

June 18, 2018

Town Council Meeting (Regular Meeting)

1. Call to Order

Mayor Myers called the meeting to order at 7:00 p.m.

2. Flag Salute

3. Roll Call:

PRESENT: Mayor Myers and Council members Boget, Bryant, Moseley, Rowe

ABSENT: Noble

PRESENT: Clerk Salisbury, Assistant Clerk Younce, Public Works Director Ross, Attorney Ridenour, Town Engineer Devin Jackson

MOTION: Council Member Boget made a motion to excuse Council member Noble's absence.

SECOND: Council member Moseley

AYES: Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion carried

4. Minutes of the Previous Meeting:

Draft minutes were presented for the June 4th, 2018 regular meeting

MOTION: Council member Bryant moved to accept the minutes of the June 4th, 2018 regular meeting.

SECOND: Council member Boget

AYES: Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion Carried

5. Late Changes to the Agenda:

Add Backroads car show to item B under new business

6. Citizen Communication:

Haley Coop- Minor girls softball players representative stated her team made it to state playoffs and are looking for donations to help pay for the trip. This is the first time this league has made it to the state playoffs since 1986. They are offering a car wash Sunday June 17th at Les Schwab in Battle Ground from 10am till they run out of cars. Also offering spaghetti feed tentatively to be held July 8th at Yacolt Community church. Time to be announced at a later date. Council Boget asked Council if there would be a problem setting up donation stations manned by NCLL minor girls players with adult supervision at the sidewalk chalk contest. Since this is considered private donations they were ok'd to set up donation stations if they would like. Haley is to get all the information to the Clerks office and Clerk will publish on Town's website and possibly community board if space is available. Mayor congratulated them on making it to state.

Dave Barton- asking permission again this year to hold 5th annual 4th of July Community BBQ with street closures at Twin Falls and Hubbard. Mr. Barton has already contacted sheriff's office and fire department for their approvals and will be obtaining and providing Clerk's office with a copy of his liability insurance. Council member Rowe asked if they would be shooting off fireworks and if they would be cleaned up. Mr. Barton said yes and assured her they would be cleaned up properly. Council approved BBQ.

Michael Leonard- Michael Leonard introduced himself and his wife Suzanne Logan as the new point of contact for NCLL. All communication for NCLL will be directed to Michael and his wife. Mr. Leonard gave an update on the girls softball tournament. Tournament is going great and he thanked KWRL for giving up their field time for this tournament. Mr. Leonard is hoping next year there will be better planning and scheduling to accommodate all parties involved.

Mr. Leonard addressed Council member Boget's letter specifically related to the broken glass and garbage issue. They have started cleaning up all areas of concern and put up a fence around containers to help deter kids from playing back there. They are starting a clean-up crew to take care of remaining issues and any future issues. They have fixed the gutter hanging down on bathrooms.

Mr. Leonard asked if there were going to be fireworks show and parade. Mayor Myers stated fireworks show is on unless cancelled by fire department due to fire danger. He also confirmed parade for July 4th at 10 am.

Mr. Leonard stated that NCLL president has been in contact with president of KWRL and their talks have been going very well. He thought that moving forward they will be able to work together on scheduling and solving any other issues that may arise.

Mr. Leonard requested any and all of the Towns records involving NCLL for the last 20 years if possible. He was informed to fill out a public records request for any information they are seeking and we will make it available to them. Mr. Leonard asked if NCLL will be given preferential treatment when making schedule for play. Mayor Myers stated he hoped NCLL and KWRL can work out schedule together. Town does not want to be involved in scheduling unless they cannot come to agreement then the Town would be the mediator as we are the ultimate arbiter as the owner of the property.

7. Old Business:

- A. Resolution #568 Use Agreement KWRL: Council member Boget verified that the 2 tax lot numbers for field 4 and ingress and egress were added to agreement. Assistant Clerk Younce agreed that they were added. Council member Bryant asked if there was anything in agreement concerning scheduling. Assistant clerk Younce stated there was not and Mayor Myers stated that there was reasonable expectations that the two parties could and should work out their respective schedules. Council member Bryant asked about any stipulations in agreement about materials to be used on fields. Assistant clerk Younce stated there were no such stipulations added to the agreement.

MOTION: Council member Bryant moved to accept the revised KWRL agreement and allow the Mayor to sign agreement.

SECOND: Council member Rowe

AYES: Council members Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion Carried

- B. Public Hearing – Amboy Ave Short Plat

Mayor Myers opened public meeting. Clerk Salisbury swore in all parties wishing to speak. David Ridenour Town Attorney clarified map to be used for presentation. Town Engineer Devin Jackson presented information why a Conditional Use Permit is needed for approval. Devin Jackson provided a brief summary of Commercial zoning in that area. Proposed permit would turn 1.3 acres into 3 single family lots. Previous property in this area has already been turned into residential with an approved conditional use permit. Devin Jackson presented staff report on the short plat with conditions if conditional use permit is approved. Council member Bryant and Boget asked for clarification on why the northerly proposed access was not recommended and why shared driveway was recommended. Byron Jolma with Bryon Jolma Design represented himself as the designer and also represented the

developer. He thanked the staff for their hard work and also asked the council to consider the previous councils commitment to the approval of the conditional use permit. He stated aesthetically 3 residential homes would look better than a large commercial parking lot. More discussion ensued about the shared driveway and width of said driveway. Devin Jackson agreed with Jolma on shared driveway option being the way to go. Jolma stated that utilities will be trenched with directional drilling so as not to tear up Amboy Avenue with trench cuts. Bill Ross brought up that a gravel driveway was proposed. He proposed that paved driveway be added to stipulation. Landscaping requirements were discussed and clarified. Council member Boget voiced concerns about how the proposed development would monetarily benefit the town over leaving it zoned commercial. Other comments were made by audience members who were not sworn in so they are not part of the official record. Clarification was made by Devin Jackson on stating C2 zoning includes zoning for multifamily housing so single family housing shouldn't be a concern in that commercial zone. Mayor Myers invited anyone wishing to speak for the project to approach podium. No speakers for project. Mayor Myers invited anyone wishing to speak against the project to the podium. No speakers against the project. Mayor Myers read statement by absent Council member Noble that is attached to these minutes. Mayor Myers stated that he left comments about the project in council packet and stated any commercial investments in town were not happening because the town is not on sewage system and they are not doing any studies on sewage system probability. Council member Moseley stated Yacolt was a great place to live and was happy to have 3 more houses available to citizens. Council member Boget voiced concerns over monetary value of giving up commercial zone for residences. She did not see how 3 residences would benefit the town more than leaving it commercial. Once property is approved commercial you can't turn it back. Mayor Myers closed public hearing and re-opened the regular Council meeting. More discussion concerning permitted businesses in that particular zone. Council member Boget read a portion of title 18.40.060 paragraph 2 citing that she didn't know if adding 3 houses to this zone is more beneficial than commercial. She didn't see it as detrimental just not beneficial. Jolma stated that there are future opportunities to change zoning codes to acquire more commercial if needed in the future. Devin Jackson supplied more clarification on future zone changes. Reminded council we are under building moratorium due to not being on sewer system. The town is regulated to use existing town boundaries for zone changes. Mayor Myers asked for motion.

MOTION: Council member Boget made motion to deny Conditional use permit application.

SECOND: Council member Rowe

AYES: Boget and Rowe

NAYES: Mosely and Bryant

ABSENT: Council member Noble

Mayor Myers voted Naye as tie breaker. Motion defeated.

MOTION: Council member Mosely made motion to table application for further review. She asked for further evidence of what kind of tax base these 3 homes will bring to the community.

SECOND: Council member Bryant

AYES: Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion carried. Add to next meeting agenda

C. Public Hearing – Jones St. Short Plat

Mayor Myers opened public meeting. Clerk Salisbury swore in all parties wishing to speak. Devin Jackson presented staff report on the short plat application with conditions. Byron Jolma represented developer. Invited any questions. Neighbor questioned tree issue. Trees have been removed. Jolma asked council to consider using earlier code BMP's used at Yacolt Crossings concerning critical aquifer recharge area for drainage. Mayor Myers invited speakers in favor. None. Mayor Myers invited speakers against. None. Mayor Myers adjourned public hearing. Mayor Myers reopened regular council meeting. Council member Bryant stated that the proposed development was in correct zone and saw no issues with application. Council member Boget concurred.

MOTION: Council member Bryant made motion to approve Jones St short plat application with conditions.

SECOND: Council member Rowe

AYES: Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion carried.

D. Public Hearing – 6 Year Transportation Plan

Mayor Myers opened public hearing. David Ridenour gave short presentation on what the 6 year transportation plan entailed. Only addition to plan was adding engineering review and planning of towns streets for 2019. Gave overview of funding options and what projects are covered under the transportation plan. Town citizen brought up problem with speeding on Jones Street and requested speed bumps be installed. Public works and Mayor stated that a 4 way stop is being

considered at that intersection. More discussion concerning children on golf carts driving on public streets. Public hearing was closed and regular council meeting reopened.

MOTION: Council member Bryant made motion to adopt 6 year transportation plan as presented by staff.

SECOND: Council member Boget

AYES: Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion carried.

E. Executive Session

Mayor Myers called for executive session. _Executive session was called to start at 8:50 pm and last 15 minutes to 9:10pm. Mayor Myers called regular council meeting back to order at 9:10 pm.

8. New Business

A: Chelatchie Prairie Railroad - Doug Auberg gave over view of new maintenance facility they want to build on county property behind Elwood short plat. He described building design and what would be happening at facility. Gave overview of past and upcoming rail events. Doug to get together with Clerk Salisbury concerning conditional use permit application.

B: Backroads for Car show: Mayor Myers read email statement asking for permission to close streets for car show August 18th. Council discussed and approved with conditions set forth in email.

9. Mayor's Comments:

Mayor Myers attended the patriotic flag contest at Fort Vancouver Park. He did not win. Property owner at the end of Jones Street that had street light removed by Clark PUD due to nonpayment of electric bill is responsible for paying to have it put back as the town had nothing to do with its removal.

10. Attorney's Comments:

None

11. Council Comments: Council member Boget gave update on Clark County Firework policy for 4th of July holiday. Stated county voted for unincorporated Clark County to go to 7 days of sales and 1 day of use starting in 2019. Council member Bryant stated Big Foot

fun run is coming up and we need more volunteers for water stations. Stated we could use minors at water stations as long as there was an adult present. Council member Moseley stated she went to CDBG grant meeting but it was about HUD funding so it did not pertain to the town.

12. Public Works Report: Bill Ross enquired about fun run signs. Council member Bryant stated she was working on them and would get them done in time. She is also picking up donations for water and Gatorade. Terry Gardner updated on getting in touch with Ken to prepare the logs for the Welcome to Yacolt signs. Terry will deliver lumber to Ken, who will peel and prepare logs and hopefully we can get them installed by June 30th.

13. Town Clerk Report: Assistant clerk Younce brought up need for volunteers for Big Foot Run June 30th. Asked which council members would be in attendance for 4th of July parade. Council member Boget and Noble will be absent. Asked council members to donate candy for the parade. Council member Boget asked if she could purchase chalk for the sidewalk contest and sell at cost. Clerk Salisbury brought up estimate for BIAS advanced payroll upgrade. Gave benefits of upgrading. Council approved cost to upgrade to advanced payroll. Had small discussion concerning electronic content management and what it entailed.

MOTION: Council member Moseley made motion to approve BIAS advanced payroll upgrade.

SECOND: Council member Boget

AYES: Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

VOTE: Motion carried.

14. Pay Bills on behalf of the Town:

MOTION: Council member Rowe moved to pay the bills on behalf of the Town.

SECOND: Council member Bryant

AYES: Council members Boget, Bryant, Moseley, Rowe

ABSENT: Council member Noble

Vote: Motion Carried

15. Adjourn:

Mayor Myers adjourned the meeting at 9:50 p.m.

DRAFT

Vince Myers, Mayor

Current Expense	23,926.23
Streets	1,352.67
Cemetery	0
REET	0
Storm Water	0
Claims	25,278.90
Payroll	0

DRAFT

Dawn Salisbury, Clerk

To the Town of Yacolt, WA Council,

Ladies and Gentlemen,

My name is Richard Dietel, along with my wife Cindy, we are local business owner and property owner.

We would like to voice our opposition to the proposed conversion of commercial property to residential property located at SE corner of Amboy ave and W. Christy. Also referred to Elwood short plat.

We feel this is not is the best interest of the town. Our concerns are the town has very limited commercial property available, and once it's gone we cannot get it back. Building residential homes right next to a main arterial road raises some safety concerns. We also feel that removing the large trees will also detract from our small-town appeal.

Regards,

Richard and Cindy Dietel



TOWN OF YACOLT

Request for Council Action

Proposed Meeting Date:

CONTACT INFORMATION FOR PERSON/GROUP/DEPARTMENT REQUESTING COUNCIL ACTION	
Name: Laura Ellsworth	Group Name: Council for the Homeless
Address: Click here to enter text.	Phone: Click here to enter text.
Email address: Click here to enter text.	Alternate Phone: Click here to enter text.

ITEM TITLE:
Action Requested of Council: Information Only
Proposed Motion: Click here to enter text.
Summary/background: Ms. Ellsworth would like todo a presentation for the Council about the Council for the Homeless. The presentation will last 20 – 30 minutes
Staff Contact(s): Assistant Clerk

AGREEMENT FOR SERVICES

January 20th, 2015

This Agreement for Services is between the Town of Yacolt, (Jurisdiction) and IBCC – International Building Code Consultants, P.C. (Contractor).

AGREEMENT:

Article I. SCOPE OF CONTRACTOR SERVICES

Section 1.01 Perform administrative services including acting in the capacity of Building Official. Perform plan reviews and inspections to verify conformance with applicable State of Washington, International Building Codes and their related standards and jurisdiction of the Town of Yacolt, Washington Titles relative to commercial and residential construction.

Section 1.02 The jurisdiction and applicant with a list of building code regulations of items needing clarification or correction to achieve compliance with applicable regulations. Each correction shall reference the applicable code section that generated the correction.

Section 1.03 Communicate with the jurisdiction and applicant to perform all necessary re-checks to achieve compliance with the jurisdictions' Titles relative to commercial and residential construction.

Section 1.04 Maintain contact with the jurisdiction to ensure compliance with the administrative requirements of the applicable codes and to ensure consistency with local policies, procedures and interpretations.

Section 1.05 Reviews for simple one and two family residences shall be returned to the jurisdiction and a check sheet sent to the applicant within five (5) working days of receipt by Contractor.

Section 1.06 Reviews for simple structural and commercial projects shall be returned to the jurisdiction and a check sheet sent to the applicant within ten (10) working days of receipt by the selected firm or individual.

Section 1.07 Rechecks for simple one and two family residences shall be performed within three (3) working days of receipt by the contractor of submitted corrections.

Article II. SCOPE OF JURISDICTION SERVICES

Section 2.01 Provide quality review at time of intake to insure the adequacy of information submitted for plan review and to be considered a complete submittal.

Section 2.02 Provide a single point-of-contact for communications and problem resolution.

Section 2.03 Collect adequate plan review fees at time of submittal to cover all contract plan review services.

Section 2.04 Coordinate site reviews to be performed by other Jurisdiction Department (e.g. storm water, traffic and transportation engineering. etc.)

Section 2.05 Coordinate review of planning and zoning requirements.

Section 2.06 Notify applicant that their project has been received by IBCC and assignment to a plan review contractor.

Section 2.07 Process and rule on any appeals generated by the project.

Section 2.08 Maintain records as required by Washington State Law.

Section 2.09 Collect all permit related fees, including Building, Plumbing, and Mechanical as required by the jurisdiction.

Section 2.10 Process contractor approved revisions and "deferred submittals" items.

Section 2.11 The jurisdiction shall have the final decision authority over plan approval and permit issuance.

Article III. COMPENSATION

Section 3.01 The Jurisdiction shall pay the Contractor (IBCC) for all work performed under this Agreement after the effective date as out below. The payment shall be full compensation for work performed under this agreement after the effective date as set out below. The payment shall be full compensation for work performed, for services rendered, and for all labor, materials, supplies, equipment and incidentals necessary to perform the work and services.

The fixed rate for residential, commercial and structural plan review services, including rechecks, meetings and consultations will be charged at 70% of the plan check fee. The fixed rate for commercial and residential building inspections, including plumbing, mechanical and structural will be charged at 70% of the building, mechanical and plumbing permit fees collected for the assigned project. The valuation shall be calculated at a minimum in accordance with Table 1A of the current addition of the International Building Code (Exhibit 1) or higher if the jurisdiction selects an alternative fee schedule.

The jurisdiction shall pay the contractor (IBCC) a bill rate of \$65.00/hour for any services with a two hour minimum for any services in which the contractor is required to perform in the capacity of the Building Official for the purpose of administrating the local Municipal Code or any other services beyond the scope of this contract.

Article IV. BILLING AND PAYMENT PROCEDURE

Section 4.01 The contractor (IBCC) shall submit to the jurisdiction a bill for payment of the compensation due. The full amount of charges for plan reviews will be due after the issuance of a plan review check sheet and, the full amount of the inspection services shall be due at the time the permit is issued. The Jurisdiction shall pay the amount due to the contractor (IBCC) within fifteen (15) days after receipt of the bill.

Article V. EFFECTIVE AND TERMINATION DATES

Section 5.01 This agreement shall be effective as of February 1st, 2015 and may be terminated at any time upon 180 days written notice by either party.

Article VI. TERMINATION OF AGREEMENT

Section 6.01 The Jurisdiction and Contractor, by mutual written agreement, may terminate this agreement at any time.

Section 6.02 The Jurisdiction or the Contractor on (180) days written notice to the other party, may terminate this agreement for any reason deemed appropriate in their sole discretion.

Section 6.03 Either the Jurisdiction or the Contractor may terminate this agreement in the event of a breach of the agreement by the other. Prior to such termination, however, the party seeking the termination shall give to the party written notice of the breach and of the party's intent to terminate. If the party has not entirely cured the breach within thirty days (30) days of notice, then the party giving the notice may terminate the Agreement at any time thereafter by giving a written notice of termination.

Article VII. PAYMENT ON TERMINATION

Section 7.01 In the event of termination, the jurisdiction shall pay the Contractor for work performed in accordance with the Agreement prior to the termination date. Any work that has been prepaid by the jurisdiction will be reimbursed to the jurisdiction. The cost to date shall be calculated at \$65.00 per hour not to exceed 70% of the permit fees.

Section 7.02 In the event of termination all Contractor's work product will become and remain property of the jurisdiction.

Article VIII. REMEDIES

Section 8.01 In the event of breach of this agreement by the Jurisdiction or the Contractor the remedy shall be limited to termination of the agreement and, receipt of payments due as per section 7.01 of this agreement.

Article IX. JURISDICTION PRIMARY CONTACT

Section 9.01 The Jurisdictions primary contact shall be the Public Works Director or any other person designated by the Jurisdiction in writing.

Article X. COMPLIANCE WITH LAWS

Section 10.01 In connection with its activities under this agreement, the Contractor shall comply with all applicable federal, state and local laws and regulations.

Article XI. LAW AND FORUM

Section 11.01 This agreement shall be construed according to the laws of the State of Washington in which the jurisdiction resides.

Section 11.02 Any litigation between the Jurisdiction and the Contractor arising under this Agreement or out of work performed under this Agreement shall occur, if in the State of Washington courts, in the County Courts having jurisdiction therefor, and if in Federal Courts, in the United States District Court for the District of Washington.

Article XII. INDEMNIFICATION

Section 12.01 The Contractor shall hold harmless, defend and indemnify the Jurisdiction and the Jurisdiction's officers, agents and employees against all claims, demands, actions and suits (including all attorney fees and cost) brought against any of them arising from the Contractor's work or by subcontractor's work under this Agreement, including payment of the just claims of all persons furnishing labor or material under this Contract. Contractor shall be considered a code enforcement agency of the jurisdiction and accorded to the maximum extent allowed by law, sovereign immunity as delineated in section 104.8 of the International Building Code 2012 edition and shown below in section 12.02 of this agreement and all associated model codes adopted by the Jurisdiction.

Section 12.02 *(International Building Code, Section 104.8 Liability) The building official, member of the board of appeals or employee charged with the enforcement of this code, while acting for the jurisdiction in good faith and without malice in the discharge of the duties required by this code or other pertinent law or ordinance, shall not thereby be rendered liable personally and is hereby relieved from personal liability for any damage accruing to persons or property as a result of any act or by reason of an act or omission in the discharge of official duties. Any suit instituted against an officer or employee because of an act performed by that officer or employee in the lawful discharge of duties and under the provisions of this code shall be defended by legal representative of the jurisdiction until the final termination of the proceedings. The building official or any subordinate shall not be liable for cost in any action, suit or proceeding that is instituted in pursuance of the provisions of this code.*

Section 12.03 To the extent permitted by law, the jurisdiction shall hold harmless, defend and indemnify the Contractor against all claims, demands, actions, and suits (including all attorney fees and cost) brought against the Contractor arising solely from the Jurisdiction's, or the Jurisdiction's officers, agents, or employees, work under this agreement.

Article XIII. WORKERS COMPENSATION INSURANCE

Section 13.01 The Contractor, its subcontractors, if any, and all employers under this Agreement are subject employees under the Washington Workers compensation law, which requires them to provide workers compensation coverage for all their subject workers. A certificate of insurance, or copy thereof, shall be attached to this Agreement, as Exhibit 2, if applicable, and shall be incorporated herein and made a term and part of this Agreement. The Contractor further agrees to maintain workers compensation insurance coverage for the duration of this Agreement.

Article XIV. ASSIGNMENT

Section 14.01 The Contractor shall not assign this Agreement, in whole or in part, or any right or obligation hereunder, without the prior written approval of the Jurisdiction.

Article XV. INDEPENDENT CONTRACTORS STATUS

Section 15.01 The Contractor is engaged as an independent contractor and will be responsible for any federal, state and local taxes and fees applicable to payments hereunder.

Section 15.02 The Contractor and its subcontractors and their employees of the jurisdiction and are not eligible for any benefits through the Jurisdiction including without limitation, federal social security, health benefits, workers compensation, unemployment compensation, and retirement benefits.

Article XVI. NOTICE

Section 16.01 Any work provide under this Agreement shall be sufficient if in writing and delivered personally to the following addressee or deposited in the United States Mail, postage prepaid, certified mail, return receipt requested, addressed as follows, or to such other address as the receiving party hereafter shall in writing:

The Jurisdiction: Town of Yacolt
 PO Box 160
 202 W. Cushman Street
 Yacolt, WA 98675

The Contractor: IBCC – International Building Code Consultants, P.C.
 Michael L Monen, Government Relations Director
 10910 NE 152nd Avenue
 Vancouver, WA 98682

Article XVII. SERERABILITY

Section 17.01 If any provision of this Agreement is found to be illegal or unenforceable, this Agreement nevertheless shall remain in full force and effect and the provision shall be stricken.

Article XVIII. INTERATION

Section 18.01 This Agreement contains the entire agreement between the Jurisdiction and the Contractor and supersedes all prior written or oral discussions or agreements.

Article XIX. FUNDS

Section 19.01 Jurisdiction certifies that sufficient funds are available and authorized for the expenditure to finance the cost of this contract.

Article XX. MAINTENANCE OF RECORDS

Section 20.01 The Contractor shall maintain records on a current basis to support its billings to the Jurisdiction and to document the performance of services in accordance with this Agreement. The Jurisdiction or its authorized representative shall have the authority to inspect, audit and copy, on reasonable notice and from time to time, any records of the Contractor regarding its billings and performance of services. The Contractor shall retain these records for inspection, audit and copying for three (3) years from the date of completion or termination of this Agreement.

Article XXI. AUDITS

Section 21.01 The Jurisdiction, either directly or through a designated representative, may conduct financial and performance audits of bills and services specified in this Agreement at any time in the course of the Agreement and during the three (3) year period established by Article XX, MAINTANCE OF RECORDS. Audits will be conducted in accordance with generally accepted auditing standards as promulgated in Government Auditing Standards by the Comptroller General of the United States General Accounting Office.

Section 21.02 If an audit discloses that payments to the Contractor under Article III, COMPENSATION and Article IV, BILLING AND PAYMENT PROCEDURE, were in excess of the amount to which the Contractor was entitled, then the Contractor shall repay the amount to which the excess to the Jurisdiction.

Article XXII. LIABILTY INSURANCE

Section 22.01 The Contractor shall maintain public liability and property damage insurance. The insurance shall provide coverage for not less than \$500,000 for personal injury to each person, \$1,000,000 for each occurrence, and \$1,000,000 for each occurrence involving property damage; or a single limit policy of not less than \$1,000,000 covering all claims per occurrence. The limits of the insurance shall be subject to changes as to maximum limits set forth in the statute liability imposed on municipality and jurisdictions of the State of Washington during the term of the Agreement. The insurance shall be without prejudice to coverage otherwise existing and shall name as additional insured the Jurisdiction and its officers, agents and employees.

Section 22.02 The insurance shall provide that the insurance shall not terminate or be canceled without thirty (30) days written notice first being given to the Jurisdiction. If the insurance is canceled or terminated prior to completion of the Agreement. The Contractor shall provide a new policy with the same terms. The Contractor agrees to maintain continuous, uninterrupted coverage for the duration of the Agreement. The insurance shall include coverage for any damages or injuries resulting out of the use of automobiles or other motor vehicles by the contractor.

Article XXIII. BREACH OF AGREEMENT

Section 23.01 The Jurisdiction or the Contractor shall breach this Agreement if it fails to perform any substantial Obligation under the Agreement, except as provided in section 23.02 of this section.

Section 23.02 Neither the Jurisdiction nor the Contractor shall have breached this Agreement by reason of any failure to perform a substantial obligation under this Agreement if the failure arises out of cause beyond its control and without its fault-or negligence. Such cases may include, without limitation, acts of God or the public enemy, acts of the federal, state or local government, fire, floods, epidemics, volcanic eruptions, quarantine restrictions, strikes, freight, embargoes and unusually severe weather. Should either the Contractor or the Jurisdiction fail to perform because of a cause described in this section, the Jurisdiction and the Contractor shall make mutually acceptable revisions.

Article XXIV. OWNERSHIP OF DOCUMENTS

Section 24.01 All work the Contractor performs under this Agreement shall be considered work made for hire and shall be the property of the Jurisdiction. The Jurisdiction shall own any and all data, documents, plans, copyrights, specifications, working papers and any other materials the Contractor produces in connection with this Agreement. On competition or termination of this Agreement the Contractor shall deliver these materials to the Public Works Director. The Contractor may retain for its own use and at its own cost copies of the materials referred to in this section.

Section 24.02 Any use the Jurisdiction makes of the material referred to in section 24.01 of this section, except for the purpose of work contemplated by this Agreement, and shall be at the Jurisdiction's risk.

Article XXV. ARBITRATION

Section 25.01 Any dispute arising out of this Agreement of the Connection with this Agreement, which is not settled by mutual agreement of the Contractor and the Jurisdiction within sixty (60) days of notification in writing by either party, shall be submitted to an arbitrator mutually agreed upon by the parties. In the event the parties can agree on the arbitrator, then the arbitrator shall be appointed by the Presiding Judge (Civil) of the Circuit Court of the State of Washington for the County of Clark. The arbitrator shall be selected within thirty (30) days from the expiration of the sixty (60) day period following notification of the dispute. The arbitrator, and any litigation arising out of or in connection with this Agreement, shall be conducted in (Clark County), shall be governed by the laws of the State of Washington, and shall be as speedy as reasonably possible. The applicable arbitration rules for the County Courts shall apply unless the parties agree in writing to other rules. The arbitrator shall render a decision within forty-five (45) days of the first meeting with the Contractor and the Jurisdiction. Insofar as the Contractor and the Jurisdiction legally may do so, they agree to be bound by the decision of the arbitrator.

Section 25.02 Not with standing any dispute under this Agreement, whether before or during arbitration, the Contractor shall continue to perform its work pending resolution of the dispute, and the Jurisdiction shall make payments as required by the Agreement for undisputed portion of the work.

Article XXVI. ADMENDMENTS

Section 26.01 The Jurisdiction and the Contractor may amend this Agreement at any time only by written amendment executed by the Jurisdiction or the Contractor. The Public Works Director or other person designated by the Jurisdiction may agree to and execute any other amendments on behalf of the Jurisdiction.

Article XXVII. NON-WAIVER

Section 27.01 The Jurisdiction and the Contractor shall not be deemed to have waived any breach of this Agreement by the other party except by an express waiver in writing. An express written waiver as to one breach shall not be deemed a waiver of any other breach not expressly identified, even though the other breach be of the same nature as that waived.

Article XXVIII. PAYMENTS TO VENDORS AND SUBCONTRACTORS

Section 28.01 The Contractor shall timely pay all suppliers, lessors and contractors providing it services, materials or equipment for carry out its obligation under this Agreement. The Contractor shall not take or fail to take action in a manner that causes the Jurisdiction or any materials that the Contractor provides hereunder to be subject to any claim or lien of any person without the Jurisdiction's prior writing consent.

Article XXIX. DEPOSIT AND RETIANER FEES

Section 29.01 It is also understood that approval of this agreement and the deposit and retainer fee of \$2,495.00 is due upon the signing of this Agreement. It is also understood that the deposit / retainer fees are 100% refundable. The refund shall be deducted from the first of all monies owed the Contractor for the services rendered under this Agreement, until the entire \$2,495.00 has been credited back to the Jurisdiction.

AGREEMENT FOR SERVICES
(Building Official / Plan Review / Building Inspections)

Town of Yacolt
Jeff Carothers, Mayor

Date: _____

ATTEST:

Clerk / Treasure

IBCC – International Building Cod Consultants, P.C.
Michael L Monen, Government Relations Director

Date: _____

TOWN OF YACOLT

Request for Council Action



Proposed Meeting Date:

CONTACT INFORMATION FOR PERSON/GROUP/DEPARTMENT REQUESTING COUNCIL ACTION

Name: DONALD GREENWALT

Group Name: [Click here to enter text.](#)

Address: [Click here to enter text.](#)

501 E. JONES ST

Phone: [Click here to enter text.](#)

360-952-1404

Email address: [Click here to enter text.](#)

Alternate Phone: [Click here to enter text.](#)

ITEM TITLE:

Action Requested of Council: [Click here to enter text.](#)

REPLACE SHED. VARIANCE ON PROPERTY
LINE SETBACKS

Proposed Motion: [Click here to enter text.](#)

Summary/background: [Click here to enter text.](#)

Staff Contact(s): [Click here to enter text.](#)

Town of Yacolt

Position Announcement

Opening Date: July 3, 2014

Closing Date: July 13, 2014

Public Works Maintenance

Title: Public Works Seasonal Help

Salary: 14.00 DOE

Department: Public Works

Reports to: Public Works Director

Status: Seasonal Part Time

General Summary:

The Public Works seasonal helper will primarily be responsible for assisting in the mowing, maintenance and upkeep of town parks, streets, buildings, stormwater systems and right-of ways. This individual must be proficient operating and maintaining equipment and be able to work outside in all weather conditions. This position reports to the Public Works Director.

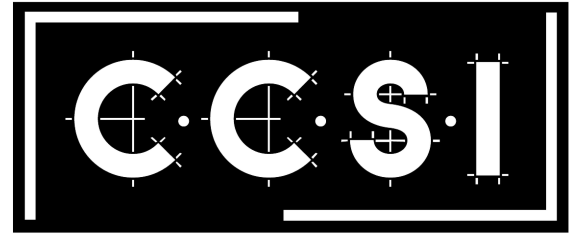
All Town employees are expected to work and act as a team player in interaction with other town employees and provide a high level of customer service to the public, other agencies, and elected officials. This individual must have education, experience, and the physical ability necessary to satisfy the job requirements. The Town of Yacolt is a drug free workplace and the candidate must be able to pass drug screening.

Information: For more information on this job, please contact Town Hall @ 686.3922 and ask for Bill or Dawn.

Application packets may be picked up at 202 W. Cushman, Yacolt, WA. 98675. Office hours are Mon-Fri, 8am – 12pm; 1pm-5pm. **** Faxed copies will not be accepted in lieu of the original application.** The Town of Yacolt requires that the original application forms be completed and received by the closing date.

*Equal Employment: The Town of Yacolt is an Equal Opportunity Employer.

Creative Computer Solutions, Inc
202 East Mill Plain Blvd
Vancouver, WA 98660
360-944-5111
www.ccsipro.com

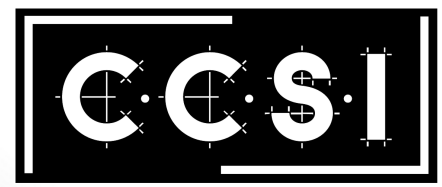


We have prepared a quote for you
CCSI | Secure Saas Firewall with central monitoring

Quote # 000999

Version 1

Town of Yacolt



Tuesday, June 26, 2018

Town of Yacolt
Dawn Salisbury
202 W Cushman
Yacolt, WA 98675
dawn.salisbury@townofyacolt.com

Dear Dawn,

I would like to take this opportunity to introduce you to Creative Computer Solutions, Inc. CCSI is a Microsoft Gold Certified Managed Services Provider offering the best available technology services to small and medium size businesses. Specializing in network infrastructure design and management, desktop | user support, remote | on-site support services, infrastructure security, e-mail | messaging management, offsite back-up and disaster recovery back-up solution, asset | licensing management, vendor management, 24|7|365 technology systems monitoring, best practice documentation including systems acceptable usage policies and network topology.

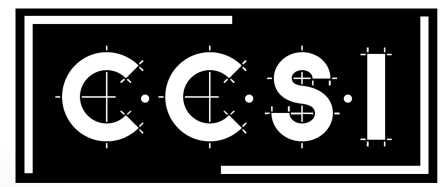
At **CCSI** our mission is simple: To accurately assess our client's technology needs and to provide the highest quality professional representation in achieving those goals. Our staff is a group of dedicated individuals focused on understanding and meeting the needs of our clients through extraordinary customer relations and providing prompt, courteous, and knowledgeable responses in a timely manner.

When you entrust your technology needs to the specialists at Creative Computer Solutions, Inc, you will see how our knowledgeable staff and timely execution of service will translate to results beyond expectation.

Enclosed, is some information about **CCSI** for your review. If you believe that Creative Computer Solutions, Inc. can be of assistance to you or your organization in the future, please give us a call.

Experience the **CCSI** difference, where we believe in ... **"Creating Clients for Life!"**

Scott Huotari
President
Creative Computer Solutions, Inc



Executive Summary

CCSI | Secure

Firewall and Content Protection

A fully managed Perimeter Firewall Solution

How It Works

There is no upfront cost to you to start the CCSI | Secure Preferred Agreement.

Our system monitors your Firewall Hardware and network traffic. Your firewall will be updated to the latest in available firmware to help detect and prevent attack. Content Filtering and Monitoring software will be installed on your firewall and will watch each packet of information for viruses, malware and other known and sometimes unknown attacks.

This plan provides the hardware for your use on a monthly basis. The CCSI | Secure Preferred plan is very flexible.

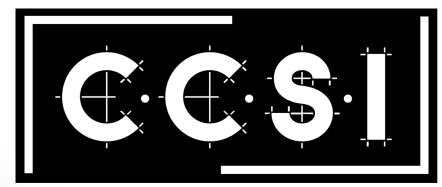
After the first 12 months we can upgrade your firewall to other models with minimal change in agreement cost. This allows your company to grow without having the cost of purchasing an entirely new firewall device.

Network Firewall Security in one simple package

Understanding network security can be complicated, but ensuring that your network is secure from malicious threats shouldn't be. CCSI |Secure Leverages the Dell SonicWALL™ Comprehensive Security Suite (CGSS) and removes the complexity associated with choosing a host of add-on security services by integrating all the network security services required for total protection into a convenient, affordable package that turns any Dell SonicWALL network security appliance into a complete Next-Generation Firewall solution.

CCSI Secure includes the following:

- Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control* Service subscription
- Content Filtering Service subscription – Premium Edition on E-Class NSA, NSA and TZ Series
- 24x7 Support subscription – E-Class Support 24x7 on E-Class products and Dynamic Support 24x7 on all others



- Central Monitoring of your device by the CCSI | NOC help desk
- Ability to upgrade your hardware device after 12 months of the agreement has occurred with minimal increase in agreement costs
- Remote support and remediation of issues related the the operation of your firewall

CCSI Secure does not include the following:

- Onsite Support of the firewall appliance

CCSI Secure optional services include the following:

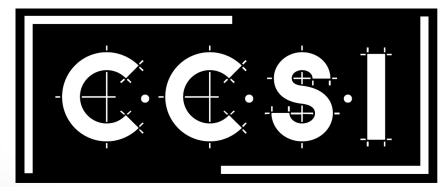
- Sonicwall Capture. This is a download sandbox that will protect your network against downloads of malicious items into your network. It is listed as an optional component to this quote.

CCSI |Secure and the Content Filtering Gateway Security Services keep your network safe from viruses, spyware, worms, Trojans, intrusion attacks and other online threats. As soon as new threats are identified and often before software vendors can patch their software, the Dell SonicWALL security solutions are automatically updated with signatures that protect against these threats and stop attacks before they can make their way into your network, ensuring you have around-the-clock protection. Your Dell SonicWALL solution also has the ability to manage internal access to inappropriate, unproductive and potentially illegal web content with comprehensive content filtering. Finally, this powerful services bundle also includes around-the-clock technical support, crucial firmware updates and real-time reporting capabilities.

Labor for remediation, upgrade, configuration is covered under the terms of our CCSI | Select, CCSI | Preferred agreements under their individual terms of service.

Secure Content Filtering Gateway Security Services at a glance

- Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention, Application Intelligence and Control Service
- Real-time gateway anti-virus engine that scans for viruses, worms, Trojans and other Internet threats in real-time
- Dynamic spyware protection blocks the installation of malicious spyware and disrupts existing spyware communications
- Powerful intrusion prevention protects against an array of network-based threats such as worms, Trojans and other malicious code
- Application intelligence and control provides application classification and policy enforcement
- Dynamically updated signature database for continuous threat protection
- Content Filtering Service (CFS)
- Comprehensive content filtering provides control of internal access to inappropriate, unproductive and potentially illegal web content
- Web site ratings cached locally on Dell SonicWALL network security appliances make response time to frequently visited sites virtually instantaneous
- Dynamically rate pages that are not in the database and automatically populate the database for future access. Only available



in Content Filtering Service Premium Edition

- Software and firmware updates and upgrades maintain network security to keep your solution as good as new

Higher performance protection

Many consumer-grade solutions lack the processing power and security sophistication to scan traffic for all threats without slowing down the network. Unlike these consumer solutions, the CCSI | Secure models utilize patented Dell SonicWALL Reassembly-Free Deep Packet Inspection® (DPI) technology to examine traffic simultaneously across all ports without introducing latency to the network. As a result, organizations are not required to make a choice between advanced DPI security and network performance. With the CCSI | Secure Firewalls, they can have both.

CCSI Secure Global Management

Statistics and Metrics from your firewall are aggregated and sent in to our Central Monitoring server where they are analyzed for trends and threats. Should an outbreak occur, we can often detect and block them before your firewall is attacked or threatened.

CCSI Secure Global Management System (GMS)p provides a powerful solution to centrally manage and rapidly deploy firewall, anti-spam, backup and recovery, and secure remote access solutions. Flexibly deployed as software, hardware, or a virtual appliance, CCSI Secure GMS offers centralized real-time monitoring, and comprehensive policy and compliance reporting. The Solution streamlines security policy management and appliance deployment, minimizing administration overhead. We can now simplify the security management of for added redundancy and scalability.

FAQ

Will the firewall slow down my network?

No, the Firewalls we put in place have enough horsepower to inspect your network traffic and keep up with your ISP provided speed.

How often will you replace my firewall device?

Under the CCSI | Secure Select Plan, we replace your hardware every 3 years automatically. If you need to upgrade due to a change in your company needs, we can upgrade your device with minimal change in the cost of this agreement.

How much will updates, upgrades and changes cost me?

The CCSI | Secure system includes all updates, firmware installation and content filtering changes to your firewall device.

With this new firewall, will I still need Virus Protection on our computers?

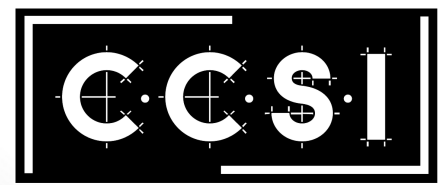
Yes. You will always need virus protection on your Servers, computers and other devices. A firewall can only limit the exposure of an attack. No system is 100% capable of preventing viruses and malware. So the more ways you have to detect a virus, the better.

What if we do get a virus on our network? Is that expense covered?

The CCSI | Secure Preferred Plan does not cover remediation of viruses. CCSI has other plans we offer that would cover that type of event.

How does CCSI | Secure protect against the Kryptolocker family of viruses?

If a server or workstation gets infected with a Kryptolocker type of virus, the Content Gateway Security Service (CGSS) service will help prevent the program (virus) from getting its encryption key from the internet.



CCSI | Secure SaaS Firewall with central monitoring

Quote Information:

Quote #: 000999
Version: 1
Delivered: 06/26/2018
Expires: 07/18/2018

Prepared for:

Town of Yacolt
Dawn Salisbury
202 W Cushman
Yacolt, WA 98675
dawn.salisbury@townofyacolt.com
(360) 686-3922

Prepared by:

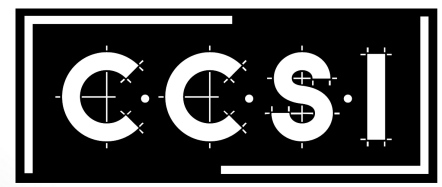
Creative Computer Solutions, Inc
Scott Huotari
360-944-5111
scott@ccsipro.com



Services		Price	Qty	Ext. Price
1	Implementation	\$1,323.00	1	\$1,323.00
Remote	Purchase and procurement		1	
Remote	Create checklist		1	
Onsite	Install and configure SonicWALL		2	
Onsite	Install and Configure SonicPoint		1	
Onsite	Add to GMS per Best Practice		1	
Remote	Update documentation and SISP		1	
Services Subtotal				\$1,323.00

Managed Services		Recurring	Qty	Ext. Recurring
	SonicWALL TZ500 Firewall-as-a-Service TotalSecure and GMS bundle subscription	\$117.00	1	\$117.00
NEW	Optional: Sonicwall Capture Service for TZ500 SonicWall Capture, a cloud based service available with SonicWall firewalls, revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unknown and zero-day attacks at the gateway, and with automated remediation. Customers benefit from high security effectiveness, fast response times and reduced total cost of ownership. Multi-engine advanced threat analysis SonicWall Capture extends firewall threat protection to detect and prevent zero-day attacks. The firewall inspects traffic and detects and blocks known malware and	\$31.00	1	\$31.00

Managed Services	Recurring	Qty	Ext. Recurring
<p>intrusions. Suspicious files are sent to the SonicWall Capture cloud service for analysis. The multi-engine sandbox platform includes virtualized sandboxing, full system emulation, and hypervisor-level analysis technology. It executes suspicious code and analyzes behavior, thus providing comprehensive visibility to malicious activity, while resisting evasion tactics and maximizing zero-day threat detection.</p> <p>Broad file type analysis</p> <p>SonicWall Capture supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK. Plus, it supports multiple operating systems, including Windows, Android, and Mac OSX environments. Administrators can customize protection by selecting or excluding files to be sent to the cloud for analysis, including by file type, file size, sender, recipient and protocol. In addition, administrators can manually submit files to the cloud service for analysis.</p> <p>Block until verdict</p> <p>To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.</p> <p>Rapid deployment of remediation signatures</p> <p>When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture subscriptions to prevent follow-on attacks. In addition, the malware is submitted to the SonicWall threat intelligence team for further analysis and inclusion of threat information into the Global Response Intelligent Defense Network (GRID) Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.</p>			



Managed Services		Recurring	Qty	Ext. Recurring
	Reporting and alerts SonicWall Capture provides an at-a-glance dashboard and reports that detail the analysis results for files sent to the service, including session information, OS information, OS activity, and network activity. Firewall log alerts provide notification of suspicious files sent to the SonicWall Capture service for analysis and results.			
	SonicWall SonicPoint ACI with PoE Injector Firewall-as-a-Service Subscription	\$32.00	1	\$32.00
Managed Services Recurring Subtotal				\$180.00

Quote Summary		Amount
	Services	\$1,323.00
	Total	\$1,323.00

Recurring Expenses Summary		Amount
	Managed Services	\$180.00
	Recurring Total	\$180.00

Pricing stated is on a monthly basis. Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors. Please refer to Appendix for additional terms and conditions.

CCSI MSP Terms and Conditions

Cancellation

CCSI requires 60 days notification in writing in the event that The Client requests cancellation of this service level agreement. The Client will be provided sixty days notification in writing in the event that CCSI requests cancellation of this service level agreement. CCSI maintains ownership of the rental equipment. Equipment will need to be returned on the day of termination of the agreement. Client agrees that this agreement is a 36 month agreement that begins on the first day of installation of the rental equipment. CCSI requires 60 day notice of cancellation of this agreement.

Upon Termination of this agreement CCSI will create a final invoice for the remaining 36 month term.

Billing/Renewal

The Client will be billed the fifth day of each month in advance for the upcoming months MSP Agreement. Payment is due by the fifteenth day of the billing month. Client will be assessed a travel charge per service call outside the standard service area which will be billed monthly according to contracted rate. This contract will automatically renew at the end of the managed service period and subsequently each term thereafter with a five percent rate increase until such time that either party notifies the other party of their wish to terminate contract or a new contract is established. Request to terminate contract requires 60 days notification in writing. For your convenience, CCSI can accept payment via all major credit cards. A 3% processing fee as charged by the credit card company will be added to the payment at the time of processing.

If it becomes necessary for Creative Computer Solutions, Inc. to travel on behalf of The Client throughout the term of this contract, all charges accrued by Creative Computer Solutions, Inc. for travel will be billed to The Client. Such items may include but are not limited to mileage, lodging, meals, and airfare. All such expenses will be preauthorized by The Client and billed to client promptly.

Force Majeure

In the event of a strike, act of God, or civil disturbance prevents Creative Computer Solutions, Inc. or The Client from performing this contract; the contract shall terminate immediately without liability to the other party.

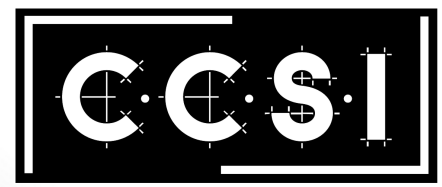
Confidentiality

Creative Computer Solutions, Inc shall treat all Client files and data as confidential and shall take all reasonable steps to ensure the staff and sub-contractors of Creative Computer Solutions, Inc observe this policy. No information reviewed by any employee, consultant, or agent of Creative Computer Solutions, Inc will be shared or provided to any outside source without prior written approval by The Client.

The Client agrees to limit access to their computer network to those employees or consultants who require such access in order to use the computer network in furtherance of The Client's business. The Client shall take all reasonable precautions to maintain the confidentiality of the computer network.

Joint management Responsibility

Both Creative Computer Solutions, Inc and The Client share responsibility for work management and oversight. Designated managers from both organizations will meet on a mutually defined regular basis to review business priorities and directions, key business milestones, work priorities, and shared work assignments. Designated managers from both Creative Computer Solutions, Inc and The Client will also be responsible for ensuring that high priority work is being addressed on a timely basis and that all key requirements are being met. Designated managers will be responsible for fully communicating issues and concerns and for ensuring that all team members are properly instructed on actions that need to be taken and corrections that need to be made. Designated managers will also be responsible for ensuring that agreed upon processes and work methods are being followed and that team members are appropriately aware of their



responsibilities in carrying out their roles. Over and above these joint management responsibilities,

The Client has full and exclusive responsibility for understanding and ensuring compliance with any regulatory, legal or contractual obligations related to data held by The Client (or by Creative Computer Solutions, Inc on The Client behalf), information provided to customers and other third parties and safeguarding and security measures that may be required. Creative Computer Solutions, Inc may participate in implementing needed systems services and functions, but The Client agrees that it shall be solely responsible for the final outcomes, actions taken and results produced.

❖ **Changes, Additions, Warranties, Stipulations or Lining Out**

CCSI fees are based on an hourly rate and a combination of the time and labor required, the novelty and difficulty of the issues involved, the skill required to resolve the issues properly, the result obtained, and the fees customarily charged in our locality for similar services. The fees also depend on which member or employee of our company provides services on your behalf. The hourly rate is applied to time spent while working on any and all client projects; this may include project scope, network documentation, estimates, etc. Special Projects are presented to client as an estimate and do not constitute a fixed bid.

The warranty on all hardware, software, cabling, and peripherals supplied by CCSI, is provided by the manufacturer. Please refer to your account manager for specific warranty details.

Any changes, additions, stipulations or corrective lining out by The Client will not be binding to Creative Computer Solutions, Inc. until such additions, clauses or stipulations have been approved by means of a corrected contract or contract addendum prepared and signed by Creative Computer Solutions, Inc.

❖ **Indemnification**

Creative Computer Solutions, Inc. agrees to indemnify and hold harmless The Client and its officers, board members, employees, their heirs, and agents, from any claim, liability, loss, costs or expense (including attorney fees and other costs and expenses of litigation through and including trial and appeals) caused by the alleged or actual negligent, reckless or intentional acts or omissions of Creative Computer Solutions, Inc., its employees or agents in rendering services pursuant to this contract.

The Client agrees to indemnify and hold harmless Creative Computer Solutions, Inc. and its officers, board members, employees, their heirs, and agents, from any claim, liability, loss, costs and expense (including attorney fees and other costs and expenses of litigation through and including trial and appeals) caused by the alleged or actual negligent, reckless or intentional acts or omissions of The Client its employees or agents in rendering services pursuant to this contract.

❖ **Alternative Dispute Resolution/Attorney Fees**

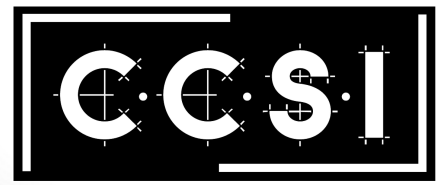
Any dispute over the interpretation or enforcement of this Agreement shall be submitted to the American Arbitration Association. The prevailing party in any dispute will be entitled to recover, in addition to all other damages provided by law, its reasonable attorney fees and costs incurred in submitting the matter to alternative dispute resolution, and if allowed, thereafter in any trial and on appeal.

❖ **Agreement in Entirety**

This agreement contains the entire agreement between the parties. Any written or verbal promises, terms, conditions, or obligations other than those contained herein that are in any manner inconsistent or contradictory to those contained herein are null and void.

❖ **Withdrawal of Offer**

This agreement / offer is considered null and void if not executed by both parties by within 30 days.



Authority to Execute Contract

It is acknowledged by the signature below that the signer has the authority from their respective organization to commit to this agreement, and sign this contract.

Creative Computer Solutions, Inc. looks forward to being of service to the staff of professionals at your company. We thank you for this opportunity and appreciate your consideration.

Signature

Date

SonicWall TZ series

Exceptional security and stellar performance at a disruptively low TCO

The SonicWall TZ series of Unified Threat Management (UTM) firewalls is ideally suited for any organization that requires enterprise-grade network protection.

SonicWall TZ series firewalls provide broad protection with advanced security services consisting of on-box and cloud-based anti-malware, anti-spyware, application control, intrusion prevention system (IPS), and URL filtering. To counter the trend of encrypted attacks, the TZ series has the processing power to inspect encrypted SSL/TLS connections against the latest threats. Combined with Dell X-Series switches, selected TZ series firewalls can directly manage the security of these additional ports.

Backed by the SonicWall Global Response Intelligent Defense (GRID) network, the SonicWall TZ series delivers continuous updates to maintain a strong network defense against cybercriminals. The SonicWall TZ series is able to scan every byte of every packet on all ports and protocols with almost zero latency and no file size limitations.

The SonicWall TZ series features Gigabit Ethernet ports, optional integrated 802.11ac wireless*, IPSec and SSL VPN, failover through integrated 3G/4G support, load balancing and network

segmentation. The SonicWall TZ series UTM firewalls also provide fast, secure mobile access over Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X and Linux platforms.

The SonicWall Global Management System (GMS) enables centralized deployment and management of SonicWall TZ series firewalls from a single system.

Managed security for distributed environments

Schools, retail shops, remote sites, branch offices and distributed enterprises need a solution that integrates with their corporate firewall. SonicWall TZ series firewalls share the same code base—and same protection—as our flagship SuperMassive next-generation firewalls. This simplifies remote site management, as every administrator sees the same user interface (UI). GMS enables network administrators to configure, monitor and manage remote SonicWall firewalls through a single pane of glass. By adding high-speed, secure wireless, the SonicWall TZ series extends the protection perimeter to include customers and guests frequenting the retail site or remote office.



Benefits:

- Enterprise grade network protection
- Deep packet inspection of all traffic without restrictions on file size or protocol
- Secure 802.11ac wireless connectivity using integrated wireless controller or via external SonicPoint wireless access points
- SSL VPN mobile access for Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS and Linux devices
- Over 100 additional ports can be securely managed by the TZ console when deployed in combination with Dell X-Series switches

* 802.11ac currently not available on SOHO models; SOHO models support 802.11a/b/g/n

SonicWall TZ600 series

For emerging enterprises, retail and branch offices looking for security performance at a value price, the SonicWall TZ600 next-generation firewall secures networks with enterprise-class features and uncompromising performance.

Specification	TZ600 series
Firewall throughput	1.5 Gbps
Full DPI throughput	500 Mbps
Anti-malware throughput	500 Mbps
IPS throughput	1.1 Gbps
IMIX throughput	900 Mbps
Max DPI connections	125,000
New connections/sec	12,000



Power LED Test LED USB port (3G/4G WAN Failover) Link and activity Indicator LEDs



Expansion module Slot (future) Console port 8x1GbE switch (configurable) X0 LAN Port X1 WAN Port Secure power

SonicWall TZ500 series

For growing branch offices and SMBs, the SonicWall TZ500 series delivers highly effective, no-compromise protection with network productivity and optional integrated 802.11ac dual-band wireless.

Specification	TZ500 series
Firewall throughput	1.4 Gbps
Full DPI throughput	400 Mbps
Anti-malware throughput	400 Mbps
IPS throughput	1.0 Gbps
IMIX throughput	700 Mbps
Max DPI connections	100,000
New connections/sec	8,000



Power LED Test LED USB port (3G/4G WAN Failover) Link and activity Indicator LEDs



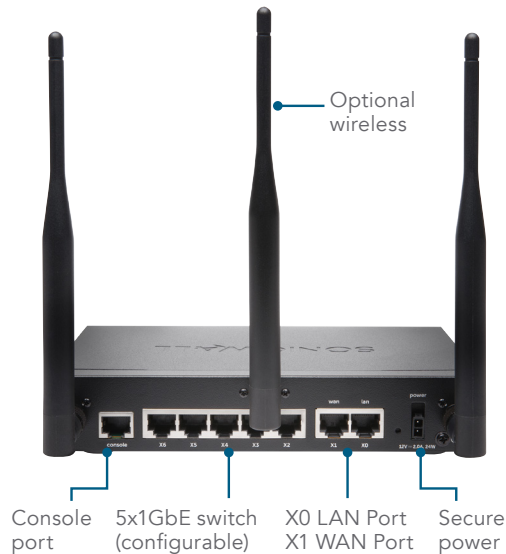
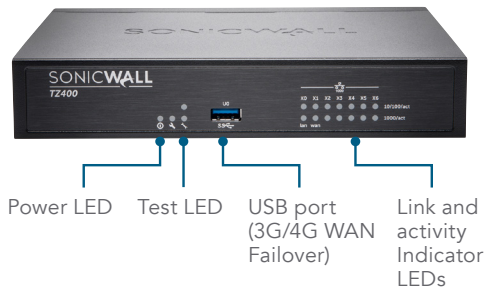
Console port 6x1GbE switch (configurable) X0 LAN Port X1 WAN Port Secure power

Optional wireless

SonicWall TZ400 series

For small business, retail and branch office locations, the SonicWall TZ400 series delivers enterprise-grade protection. Flexible wireless deployment is available with either external SonicPoint Access points or 802.11ac wireless integrated into the unit.

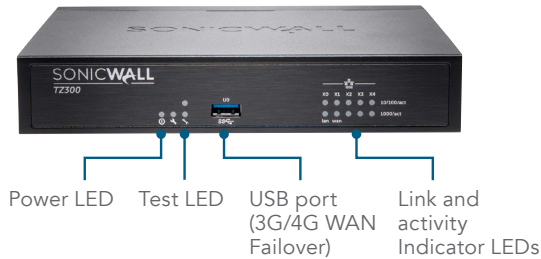
Specification	TZ400 series
Firewall throughput	1.3 Gbps
Full DPI throughput	300 Mbps
Anti-malware throughput	300 Mbps
IPS throughput	900 Mbps
IMIX throughput	500 Mbps
Max DPI connections	90,000
New connections/sec	6,000



SonicWall TZ300 series

The SonicWall TZ300 series offers an all-in-one solution that protects networks from attack. Unlike consumer grade products, the SonicWall TZ300 series firewall combines effective intrusion prevention, anti-malware and content/URL filtering with optional 802.11ac integrated wireless and broadest secure mobile platforms support for laptops, smartphones and tablets.

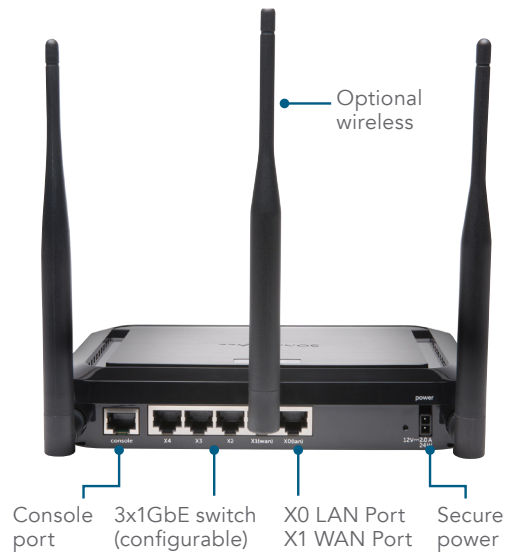
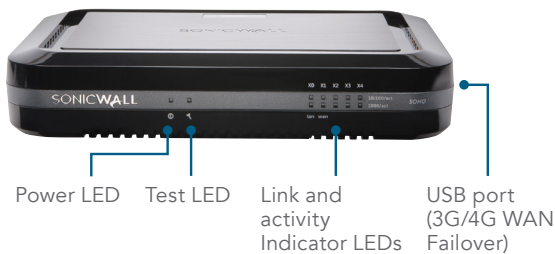
Specification	TZ300 series
Firewall throughput	750 Mbps
Full DPI throughput	100 Mbps
Anti-malware throughput	100 Mbps
IPS throughput	300 Mbps
IMIX throughput	200 Mbps
Max DPI connections	50,000
New connections/sec	5,000



SonicWall SOHO series

For wired and wireless small and home office environments, the SonicWall SOHO series delivers the same business-class protection large organizations require at a more affordable price point.

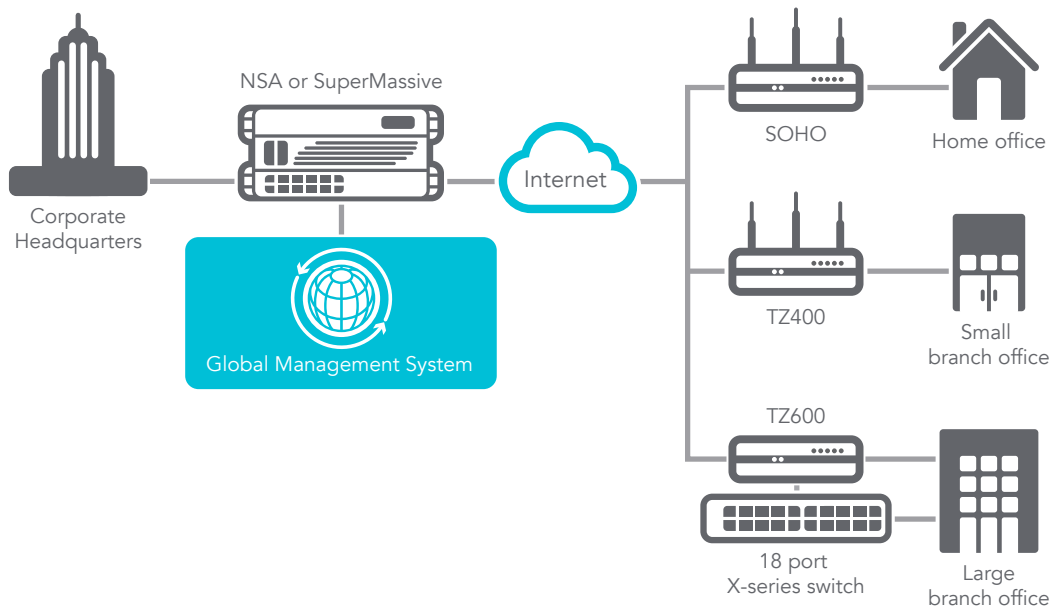
Specification	SOHO series
Firewall throughput	300 Mbps
Full DPI throughput	50 Mbps
Anti-malware throughput	50 Mbps
IPS throughput	100 Mbps
IMIX throughput	60 Mbps
Max DPI connections	10,000
New connections/sec	1,800



Extensible architecture for extreme scalability and performance

The Reassembly-Free Deep Packet Inspection (RFDPI) engine is designed from the ground up with an emphasis on providing security scanning at a high performance level, to match both the inherently parallel and ever-growing nature of network traffic. When combined with multi-core processor systems, this parallel-centric software architecture scales up perfectly to

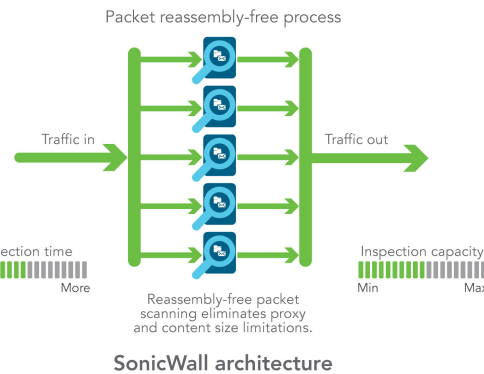
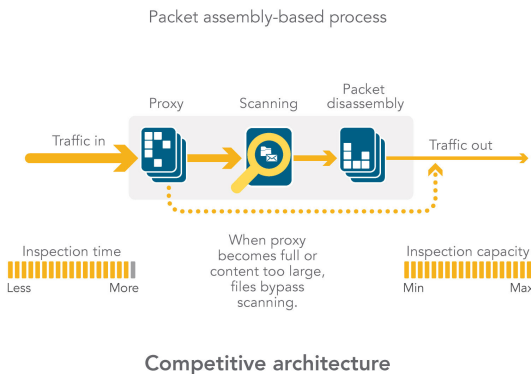
address the demands of deep packet inspection at high traffic loads. The SonicWall TZ Series platform relies on processors that, unlike x86, are optimized for packet, crypto and network processing while retaining flexibility and programmability in the field — a weak point for ASICs systems. This flexibility is essential when new code and behavior updates are necessary to protect against new attacks that require updated and more sophisticated detection techniques.



Reassembly-Free Deep Packet Inspection (RFDPI) engine

The RFDPI engine provides superior threat protection and application control without compromising performance. This patented engine inspects the traffic stream 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 preprocessing, including SSL decryption, it is analyzed against

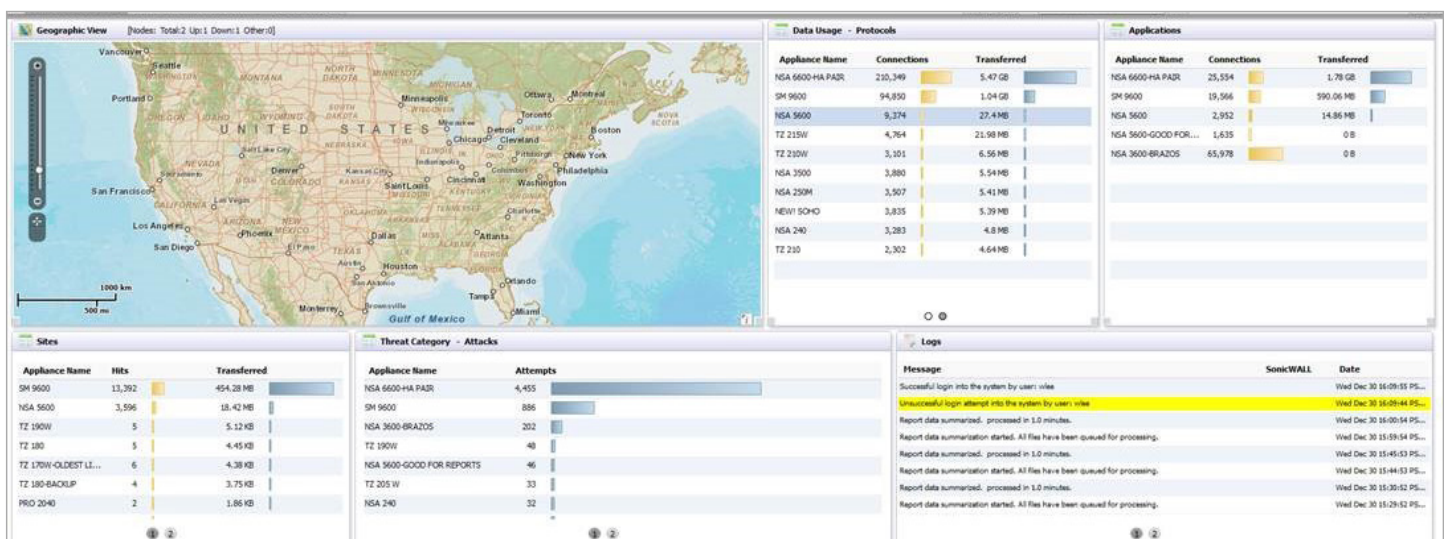
a single proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or another “match” event, at which point a pre-set action is taken. As malware is identified, the SonicWall firewall terminates the connection before any compromise can be achieved and properly logs the event. However, the engine can also be configured for inspection only or, in the 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.



Global management and reporting

For larger, distributed enterprise deployments, the optional SonicWall Global Management System (GMS) provides administrators a unified, secure and extensible platform to manage SonicWall security appliances and Dell X-Series switches. 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. 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.



Security and protection

The dedicated, in-house SonicWall Threat 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. SonicWall firewall customers with current subscriptions 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, all SonicWall firewalls also have access to the SonicWall CloudAV service, which extends the onboard signature intelligence with more than 17 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, SonicWall next-generation firewalls are able to block traffic from dangerous domains or entire geographies in order to reduce the risk profile of the network.

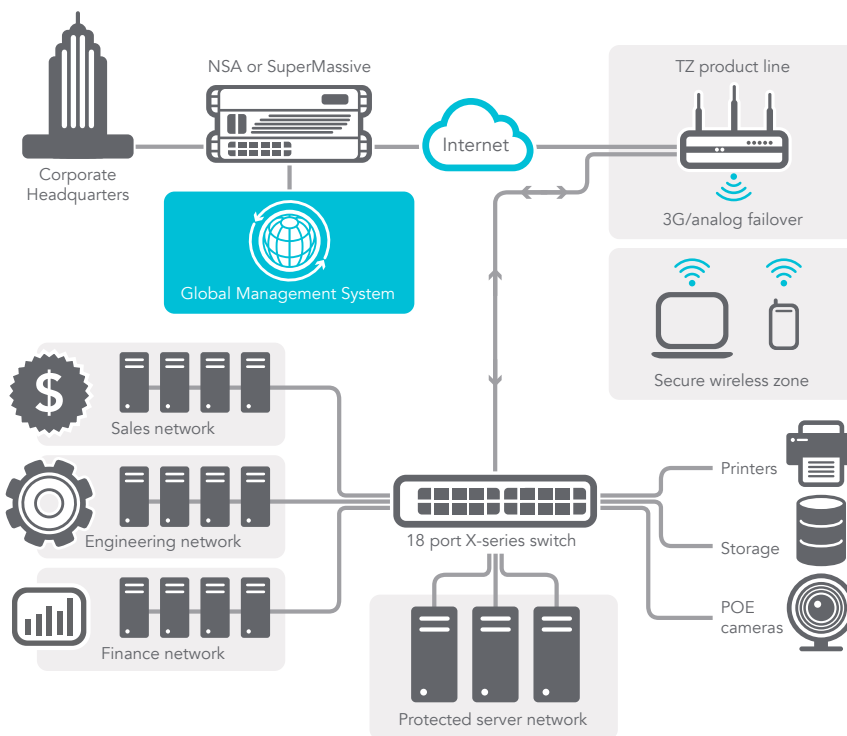
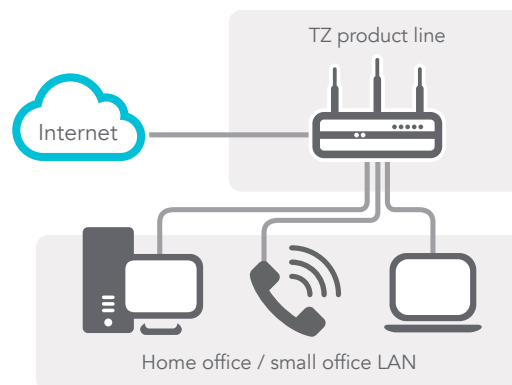
Application intelligence and control

Application intelligence informs administrators of application traffic traversing the 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. 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 enhance the user experience, increase productivity and reduce support calls. Management of application intelligence and control is simplified by using an intuitive web-based interface.

Flexible and secure wireless

Available as an optional feature, high-speed 802.11ac wireless* combines



with SonicWall next-generation firewall technology to create a wireless network security solution that delivers comprehensive protection for wired and wireless networks.

This enterprise-level wireless performance enables WiFi-ready devices to connect from greater distances and use bandwidth-intensive mobile apps, such as video and voice, in higher density environments without experiencing signal degradation.

* 802.11ac currently not available on SOHO models; SOHO models support 802.11a/b/g/n

Features

RFDPI engine	
Feature	Description
Reassembly-Free Deep Packet Inspection	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.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for deep packet inspection of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Deep Packet Inspection of Secure Socket Shell (DPI-SSH)	Detects and prevents advanced encrypted attacks that leverage SSH, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control communications and data exfiltration.
Capture Advanced Threat Protection	
Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity
Broad file type analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OSX and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture subscriptions and GRID Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Encrypted Threat Protection	
Feature	Description
TLS/SSL decryption and 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 TLS/SSL encrypted traffic. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspects data traversing over SSH tunnels to prevent attacks that leverage SSH.
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 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	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.
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 malware protection	A continuously updated database of over 17 million threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.

Threat prevention con't	
Feature	Description
SSL decryption and 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. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they 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, SMBv1/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	Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over 3,500 application signatures, to increase network security and enhance network productivity.
Custom application identification	Control 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.
Granular control	Control applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.
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.
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 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	Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	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 option	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.
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 SonicWall TZ 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, the hardware will support filtering implementations.
Biometric authentication for remote access	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user's identity for network access.
Dell X-Series switch integration	Manage security settings of additional ports, including POE and POE+, under a single pane of glass using TZ series dashboard with X series switch (not available with the SOHO model)

Firewall and networking con't	
Feature	Description
High availability	SonicWall TZ500 and SonicWall TZ600 models support high availability with Active/Standby with state synchronization. SonicWall TZ300 and SonicWall TZ400 models support high availability without Active/Standby synchronization. There is no high availability on SonicWall SOHO models.
Threat API	Enables the firewall to receive any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Wireless Network Security	IEEE 802.11ac wireless technology can deliver up to 1.3 Gbps of wireless throughput with greater range and reliability. Available on SonicWall TZ600 through SonicWall TZ300 models. Optional 802.11 a/b/g/n is available on SonicWall SOHO models.
Management and reporting	
Feature	Description
Global Management System	SonicWall GMS monitors, configures and reports on multiple SonicWall appliances and Dell X-Series switches 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. Also, a comprehensive command line interface 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 SonicWall GMSFlow Server or other tools that support IPFIX and NetFlow with extensions.
Virtual Private Networking	
Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the SonicWall TZ 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 fallback of all VPN sessions.
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/Citrix1/TerminalServices 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

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- Threat API

SSL/SSH decryption and inspection¹

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control

Capture Advanced Threat Protection¹

- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated & manual submission
- Real-time threat intelligence updates
- Auto-Block capability

Intrusion prevention¹

- Signature-based scanning
- Automatic signature updates
- Bidirectional inspection engine
- Granular IPS rule capability
- GeolIP/Botnet filtering²
- Regular expression matching

Anti-malware¹

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

Application identification¹

- Application control
- Application visualization²
- Application component blocking

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

Web content filtering¹

- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (OSPF, RIP)

Networking

- PortShield
- Enhanced logging
- Layer-2 QoS
- Port security
- Dynamic routing
- SonicPoint wireless controller
- Policy-based routing
- Asymmetric routing
- DHCP server
- NAT
- Bandwidth management
- High availability - Active/Standby with state sync³
- Inbound/outbound load balancing
- L2 bridge mode, NAT mode
- 3G/4G WAN failover
- Common Access Card (CAC) support

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
- Centralized management and reporting with SonicWall GMS
- Logging
- Netflow/IPFix exporting
- Single Sign-On (SSO)
- Terminal service/Citrix support
- Application and bandwidth visualization
- IPv4 and IPv6 management
- Dell X-Series switch management

IPv6

- IPv6 filtering
- 6rd (rapid deployment)
- DHCP prefix delegation
- BGP

Wireless

- Dual-band (2.4 GHz and 5.0 GHz)
- 802.11 a/b/g/n/ac wireless standards²
- Wireless intrusion detection and prevention
- Wireless guest services
- Lightweight hotspot messaging
- Virtual access point segmentation
- Captive portal
- Cloud ACL

¹ Requires added subscription

² Not available on SOHO series

³ State sync high availability only on SonicWall TZ500 and SonicWall TZ600 models

SonicWall TZ series system specifications

Hardware overview	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Operating system	SonicOS				
Security processing cores	2 x 400 MHz / 2 x 800 MHz	2 x 800 MHz	4 x 800 MHz	4 x 1 GHz	4 x 1.4 GHz
Interfaces	5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, 1 Expansion Slot
Memory (RAM)	512 MB / 1 GB	1 GB	1 GB	1 GB	1 GB
Memory (flash)	32 MB / 64 MB	64 MB	64 MB	64 MB	64 MB
Expansion	USB	USB	USB	2 USB	Expansion Slot (Rear)*, 2 USB
Single Sign-On (SSO) Users	250	500	500	500	500
VLAN interfaces	25	25	50	50	50
SonicPoints supported (maximum)	2	8	16	16	24
Dell X-Series switch models supported	Not available	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Firewall/VPN performance	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Firewall inspection throughput ¹	300 Mbps	750 Mbps	1,300 Mbps	1,400 Mbps	1,500 Mbps
Full DPI throughput ²	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
Application inspection throughput ²	-	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
IPS throughput ²	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Anti-malware inspection throughput ²	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
IMIX throughput ³	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
SSL inspection and decryption throughput (DPI SSL) ²	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
IPSec VPN throughput ³	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
Connections per second	1,800	5,000	6,000	8,000	12,000
Maximum connections (SPI)	10,000	50,000	100,000	125,000	150,000
Maximum connections (DPI)	10,000	50,000	90,000	100,000	125,000
SSL DPI connections	100	250	250	250	250
VPN	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Site-to-site VPN tunnels	10	10	20	25	50
IPSec VPN clients (maximum)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL VPN licenses (maximum)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual assist bundled (maximum)	-	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)	1 (30-day trial)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1, Suite B Cryptography				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14				
Route-based VPN	RIP, OSPF				
Certificate support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to- SonicWall VPN, SCEP				
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN				
Global VPN client platforms supported	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10				
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)				
Security services	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL				
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists				
Enforced Client Anti-Virus and Anti-Spyware	McAfee® and Kaspersky™				
Comprehensive Anti-Spam Service	Supported				
Application Visualization	No	Yes	Yes	Yes	Yes
Application Control	Yes	Yes	Yes	Yes	Yes
Capture Advanced Threat Protection	No	Yes	Yes	Yes	Yes

SonicWall TZ series system specifications con't

Networking	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
IP address assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay				
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode				
Routing protocols ⁴	BGP ⁴ , OSPF, RIPv1/v2, static routes, policy-based routing, multicast				
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)				
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix			
Local user database	150			250	
VoIP	Full H.323v1-5, SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	FIPS 140-2 (with Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus				
Certifications pending	Common Criteria NDPP				
Common Access Card (CAC)	Supported				
High availability	No	Active/standby	Active/standby	Active/standby with stateful synchronization	Active/standby with stateful synchronization
Hardware	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Form factor	Desktop				
Power supply (W)	24W external	24W external	24W external	36W external	60W external
Maximum power consumption (W)	6.4 / 11.3	6.9 / 12.0	9.2 / 13.8	13.4 / 17.7	16.1
Input power	100 to 240 VAC, 50-60 Hz, 1 A				
Total heat dissipation	21.8 / 38.7 BTU	23.5 / 40.9 BTU	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Dimensions	3.6x14.1x19cm	3.5x13.4x19cm	3.5x13.4x19cm	3.5x15x22.5cm	3.5x18x28cm
Weight	0.34 kg / 0.75 lbs 0.48 kg / 1.06 lbs	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.73 kg / 1.61 lbs 0.84 kg / 1.85 lbs	0.92 kg / 2.03 lbs 1.05 kg / 2.31 lbs	1.47 kg / 3.24 lbs
WEEE weight	0.80 kg / 1.76 lbs 0.94 kg / 2.07 lbs	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.15 kg / 2.53 lbs 1.26 kg / 2.78 lbs	1.34 kg / 2.95 lbs 1.48 kg / 3.26 lbs	1.89 kg /4.16 lbs
Shipping weight	1.20 kg / 2.64 lbs 1.34 kg / 2.95 lbs	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.37 kg / 3.02 lbs 1.48 kg / 3.26 lbs	1.93 kg / 4.25 lbs 2.07 kg / 4.56 lbs	2.48 kg / 5.47 lbs
MTBF (years)	58.9/56.1 (wireless)	56.1	54.0	40.8	18.4
Environment	40-105° F, 0-40° C				
Humidity	5-95% non-condensing				
Regulatory	SOHO series	TZ300 series	TZ400 series	TZ500 series	TZ600
Regulatory model (wired)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Major regulatory compliance (wired models)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, BSMI, KCC/MSIP	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL cUL, TUV/ GS, CB, Mexico CoC by UL, WEEE , REACH, KCC/MSIP
Regulatory model (wireless)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Major regulatory compliance (wireless models)	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH	-

SonicWall TZ series system specifications con't

Integrated Wireless	SOHO series	TZ300, TZ400, TZ500 series	TZ600
Standards	802.11 a/b/g/n	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS)	-
Frequency bands ⁵	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz;	802.11a: 5.180-5.825 GHz; 802.11b/g: 2.412-2.472 GHz; 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz; 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz	-
Operating Channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64;	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64	-
Transmit output power	Based on the regulatory domain specified by the system administrator	Based on the regulatory domain specified by the system administrator	-
Transmit power control	Supported	Supported	-
Data rates supported	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel;	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11b: 1, 2, 5.5, 11 Mbps per channel; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel	-
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	-

*Future use.

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/GatewayAV/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.

⁴ BGP is available only on SonicWall TZ400, TZ500 and TZ600.

⁵ All TZ integrated wireless models can support either 2.4GHz or 5GHz band. For dual-band support, please use SonicWall's wireless access points products (SonicPoints)

SonicWall TZ Series ordering information

Product	SKU
SonicWall SOHO with 1-year TotalSecure	01-SSC-0651
SonicWall SOHO Wireless-N with 1-year TotalSecure	01-SSC-0653
SonicWall TZ300 with 1-year TotalSecure	01-SSC-0581
SonicWall TZ300 Wireless-AC with 1-year TotalSecure	01-SSC-0583
SonicWall TZ400 with 1-year TotalSecure	01-SSC-0514
SonicWall TZ400 Wireless-AC with 1-year TotalSecure	01-SSC-0516
SonicWall TZ500 with 1-year TotalSecure	01-SSC-0445
SonicWall TZ500 Wireless-AC with 1-year TotalSecure	01-SSC-0446
SonicWall TZ600 with 1-year TotalSecure	01-SSC-0219
High availability options (each unit must be the same model)	
SonicWall TZ500 High Availability	01-SSC-0439
SonicWall TZ600 High Availability	01-SSC-0220

SonicWall TZ Series ordering information con't

Services	SKU
For SonicWall SOHO	
Comprehensive Gateway Security Suite 1-year	01-SSC-0688
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0670
Content Filtering Service 1-year	01-SSC-0676
Comprehensive Anti-Spam Service 1-year	01-SSC-0682
24x7 Support 1-year	01-SSC-0700
For SonicWall TZ300	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ300 (1-year)	01-SSC-1430
Capture Advanced Threat Protection for TZ300 (1-year)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0602
Content Filtering Service 1-year	01-SSC-0608
Comprehensive Anti-Spam Service 1-year	01-SSC-0632
24x7 Support 1-year	01-SSC-0620
For SonicWall TZ400	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ400 (1-year)	01-SSC-1440
Capture Advanced Threat Protection for TZ400 (1-year)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0534
Content Filtering Service 1-year	01-SSC-0540
Comprehensive Anti-Spam Service 1-year	01-SSC-0561
24x7 Support 1-year	01-SSC-0552
For SonicWall TZ500	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ500 (1-year)	01-SSC-1450
Capture Advanced Threat Protection for TZ500 (1-year)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0458
Content Filtering Service 1-year	01-SSC-0464
Comprehensive Anti-Spam Service 1-year	01-SSC-0482
24x7 Support 1-year	01-SSC-0476
For SonicWall TZ600	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for TZ600 (1-year)	01-SSC-1460
Capture Advanced Threat Protection for TZ600 (1-year)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention and Application Control 1-year	01-SSC-0228
Content Filtering Service 1-year	01-SSC-0234
Comprehensive Anti-Spam Service 1-year	01-SSC-0252
24x7 Support 1-year	01-SSC-0246

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

SonicWall, Inc.

5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

© 2017 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.
Datasheet-TZ Series-US-VG-28008



SonicWall Security-as-a-Service

Stop viruses, spyware, worms, Trojans, key loggers, and more before they enter your network, with all-in-one, comprehensive network protection. SonicWall provides you with the same level of network security that NASA demands and protects your network from a wide range of emerging threats.

Block threats before they enter your network

Entry points into your network may now include employees' laptops, desktops, and smartphones. Secure your network and data against sophisticated, modern-day threats with comprehensive protection that includes intrusion prevention, gateway anti-virus, anti-spyware, content/url filtering, enforced client anti-virus, and anti-spam services.

Eliminate bottlenecks

The amount of traffic being scanned by your firewall, as well as the increasing amount of threats and malware attacking it, is quickly becoming more than many firewalls can handle. SonicWall is designed to protect organizations of every size without slowing down your network — providing you with fast, reliable performance.

Keep your network productive

Your network performance can be bogged down by spam, unauthorized web activity and social networking traffic that have nothing to do with getting work done. Ensure your business-critical applications have the bandwidth they need with content and application control tools.

Provide secure mobile access from any platform

Your employees need access to email, files and applications wherever they are. Now you can allow mobile users to access your network with secure VPN remote access for Windows, Apple iOS, Android, Mac OS X and Kindle Fire devices and be assured that it is safe, secure, and free from threats.

Get an all-in-one solution

Combine the features of traditional firewalls, gateway anti-malware products, intrusion prevention systems and content filtering software in a single solution. All of these security technologies are installed, configured, deployed, and managed as one unit. Detailed event data is available through one reporting system so it is easier to identify threats early and take appropriate measures BEFORE your network has been compromised.

Protect your network with comprehensive security at a small business price

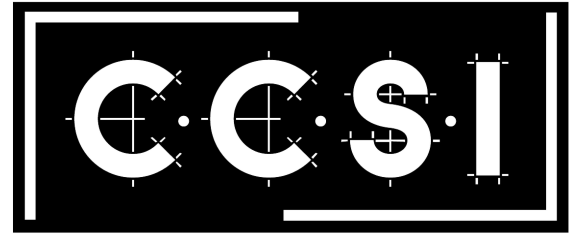
- Block viruses, Trojans, worms, rootkits and polymorphic "zero-day" malware at the gateway, before they reach your network
- Prevent "drive-by downloads" from infected websites
- Mitigate denial-of-service and flooding attacks
- Detect protocol anomalies and buffer overflow attacks
- Stop network traffic from geographical regions and IP addresses associated with cybercriminals
- Block outbound cybercriminals botnet "command and control" traffic from stealing your customer lists, engineering designs, trade secrets, and other confidential information
- Control access to websites containing unproductive and inappropriate content
- Ensure high-priority applications (CRM, order processing) receive more bandwidth than less urgent applications (chat, video streaming)

Advantages of a managed security service

- Outsource your network security to an experienced security provider
- Firewall expertly configured by SonicWall-certified engineers
- Turn-key solution delivered to your doorstep
- Proactive monitoring and alerting
- Updating of firmware, software, and security updates
- Automated weekly network and security reports
- Report analysis by SonicWall-certified engineers
- Weekly off-site SonicWall configuration backup
- Upgrade appliance as future business and technology changes dictate

Available through a
SonicWall-certified partner.

Creative Computer Solutions, Inc
202 East Mill Plain Blvd
Vancouver, WA 98660
360-944-5111
www.ccsipro.com



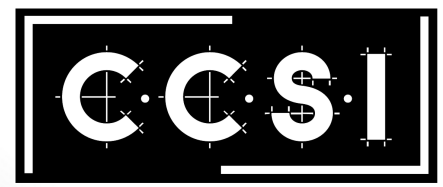
We have prepared a quote for you

CCSI Essential Plan 4

Quote # 000998

Version 2

Town of Yacolt



Tuesday, June 26, 2018

Town of Yacolt
Dawn Salisbury
202 W Cushman
Yacolt, WA 98675
dawn.salisbury@townofyacolt.com

Dear Dawn,

I would like to take this opportunity to introduce you to Creative Computer Solutions, Inc. CCSI is a Microsoft Gold Certified Managed Services Provider offering the best available technology services to small and medium size businesses. Specializing in network infrastructure design and management, desktop | user support, remote | on-site support services, infrastructure security, e-mail | messaging management, offsite back-up and disaster recovery back-up solution, asset | licensing management, vendor management, 24|7|365 technology systems monitoring, best practice documentation including systems acceptable usage policies and network topology.

At **CCSI** our mission is simple: To accurately assess our client's technology needs and to provide the highest quality professional representation in achieving those goals. Our staff is a group of dedicated individuals focused on understanding and meeting the needs of our clients through extraordinary customer relations and providing prompt, courteous, and knowledgeable responses in a timely manner.

When you entrust your technology needs to the specialists at Creative Computer Solutions, Inc, you will see how our knowledgeable staff and timely execution of service will translate to results beyond expectation.

Enclosed, is some information about **CCSI** for your review. If you believe that Creative Computer Solutions, Inc. can be of assistance to you or your organization in the future, please give us a call.

Experience the **CCSI** difference, where we believe in ... **"Creating Clients for Life!"**

Scott Huotari
President
Creative Computer Solutions, Inc

An orange graphic consisting of three hexagons arranged in a triangular pattern, with the top one being larger than the two below it.

Executive Summary

Managed Services Plan

CCSI | msp

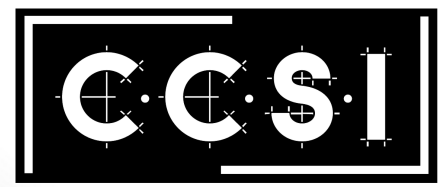
The CCSI Team saves clients invaluable time and money by making sure that your employees are productive each and every day. They depend on their computers to provide a better product to your clients, and we know that. Each of our engineers are the best at what they do and cross train each other every day on their experiences they have with our other clients. If an issue occurs on a server somewhere else, be rest assured that our best practices are being modified to make sure that those errors do not occur at your location in the future.

Our experience directly impacts your bottom line and the happiness of your employees with their computer experience.

In the past, you had to wait for a problem to occur before you could start to fix it. Today, CCSI has the latest network monitoring and management tools to foresee most network issues before they send your business to a standstill. Your employees do not have to feel the pain prior to the issues being addressed.

The CCSI Essential Service Level Agreement monthly charge includes:

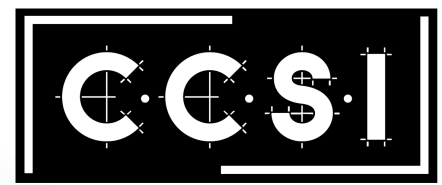
- Support from a Microsoft Gold Certified Managed Services Provider, signifying the distinction of CCSI being among the top 1% of Microsoft partners in the world.
- 24/7/365 monitoring of Desktops & Servers
- Phone/Help Desk & Onsite support is available to your designated staff
- Anti-virus & anti-spyware
- OpenDNS Web filtering Subscription for devices and perimeter security
- White List Patch Management
- Remote Access for Support Staff
- Remote Access is available for employee remote access
- Monthly, Quarterly & Annual Performance Reports
- Asset & licensing management
- Best practice documentation including systems acceptable usage policies and network topology
- Vendor Management



- Internal auditing of work performed
- Template management, client ready for security & network management, password policies

The Cost of Services NOT included in the Select Plus Service Level Agreement:

- After hours emergency support (not between 8am – 5pm Monday thru Friday) is billed @ \$223.50 per hour (1 hour minimum)
- On-site Incidental Support (after monthly MSP hour is used) is billed @ \$159.00 per hour
- Remote Help Desktop Support (after monthly MSP hour is used) is billed in 15 minute increments @ \$39.75 per ¼ hour
- Annual Desktop Maintenance is recommended
- Server maintenance is recommended at 3 hours performed quarterly per server
- Incidental help desk or onsite support
- Mileage to and from client site



CCSI Essential Plan 4

Quote Information:

Quote #: 000998
Version: 2
Delivered: 06/26/2018
Expires: 07/18/2018

Prepared for:

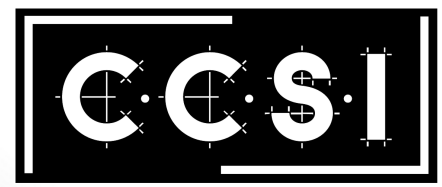
Town of Yacolt
Dawn Salisbury
202 W Cushman
Yacolt, WA 98675
dawn.salisbury@townofyacolt.com
(360) 686-3922

Prepared by:

Creative Computer Solutions, Inc
Scott Huotari
360-944-5111
scott@ccsipro.com



Managed Services		Recurring	Qty	Ext. Recurring
CCSI Essential Desktop Care	CCSI Essential Desktop Care	\$12.95	4	\$51.80
UDC	Ultimate Desktop Care Agent CCSI Ultimate Desktop Care (UDC) is an agent based system and included in this SLA. Every managed desktop or laptop must have the CCSI monitoring agent installed. The desktop agent collects system configurations, asset information (software and hardware), Microsoft patch status, S.M.A.R.T. hard drive statistics, and antivirus and anti-spyware information which are then sent to the Data Center Application. The CCSI Ultimate Desktop Care Agent is also responsible for executing patch and software deployments, uninstall routines, maintenance activities and remote control initiation. The Desktop Agent performs its responsibilities based on instructions received from the Data Center Application. CCSI Ultimate Desktop Care is provided on desktops in accordance with this SLA. Any workstations/laptops added to the network will automatically modify this contract adding the additional devices to this SLA. An adjustment to the program pricing will be made and reflected on the next month's invoice.		4	
Umbrella	CCSI Secure DNS Umbrella Services Our cloud-delivered network security uses predictive intelligence to combat the malware that antivirus and firewalls miss. Our intelligence uses machine learning to proactively protect against known and emergent threats before your staff are attacked. This decreases time spent remediating infections by as much as 80%. CCSI Umbrella simplifies proactive enterprise-level security by delivering centralized settings, reporting and management of threats. Umbrella minimizes service overhead by covering devices worldwide, on-premises and off-network, in minutes. Umbrella stays up-to-date without admin intervention because there is no hardware to install or software to maintain. The Centralized Settings feature makes it simpler to manage customer settings in bulk, so you implement changes once instead of repeating the same task for each end user or end point.		4	



Managed Services		Recurring	Qty	Ext. Recurring
File Replication	CCSI Anchor file backup and replication service. Will allow for backup of primary station. We can add additional licenses to support the council laptops as needed	\$120.00	1	\$120.00
Labor	Prepaid block of Time discounted by \$10.00 per hour as prepaid block Onsite Service blocks of time, sold at a discount rate and bundled as part of your monthly agreement. Unused hours are rolled forward. Unused hours have no cash value, but are accumulated as part of this agreement.	\$149.00	0	\$0.00
Managed Services Recurring Subtotal				\$171.80

Recurring Expenses Summary		Amount
Managed Services		\$171.80
Recurring Total		\$171.80

Pricing stated is on a monthly basis. Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors. Please refer to Appendix for additional terms and conditions.

CCSI MSP Terms and Conditions

Cancellation

CCSI requires sixty days notification in writing in the event that The Client requests cancellation of this service level agreement. The Client will be provided sixty days notification in writing in the event that CCSI requests cancellation of this service level agreement.

By agreement and understanding, there will however be an initial review date at 90 days from the start of the service contract. If, for any reason, during that period, either party is dissatisfied with the relationship, the notice of termination shall be five working days.

CCSI Ultimate Desktop Care and CCSI Server Watch provide client with antivirus and anti-spyware software protection. Contract must be valid and client in good standing for antivirus and anti-spyware software to remain active. If contract is cancelled, the antivirus and anti-spyware software will become invalid beginning the first of the month following the date of the cancellation request.

Billing/Renewal

The Client will be billed the fifth day of each month in advance for the upcoming month MSP Agreement. Payment is due by the fifteenth day of the billing month. Client will be assessed a travel charge per service call outside the standard service area which will be billed monthly according to contracted rate. This contract will automatically renew at the end of the managed service period and subsequently each year thereafter with a five percent rate increase until such time that either party notifies the other party of their wish to terminate contract or a new contract is established. Request to terminate contract requires sixty days notification in writing. For your convenience, CCSI can accept payment via all major credit cards. A 3% processing fee as charged by the credit card company will be added to the payment at the time of processing.

If it becomes necessary for Creative Computer Solutions, Inc. to travel on behalf of The Client throughout the term of this contract, all charges accrued by Creative Computer Solutions, Inc. for travel will be billed to The Client. Such items may include but are not limited to mileage, lodging, meals, and airfare. All such expenses will be preauthorized by The Client and billed to client promptly.

Force Majeure

In the event of a strike, act of God, or civil disturbance prevents Creative Computer Solutions, Inc. or The Client from performing this contract; the contract shall terminate immediately without liability to the other party.

Confidentiality

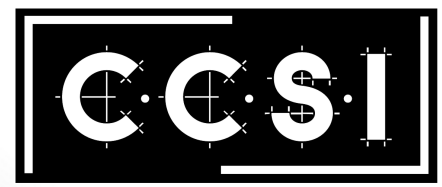
Creative Computer Solutions, Inc shall treat all Client files and data as confidential and shall take all reasonable steps to ensure the staff and sub-contractors of Creative Computer Solutions, Inc observe this policy. No information reviewed by any employee, consultant, or agent of Creative Computer Solutions, Inc will be shared or provided to any outside source without prior written approval by The Client.

The Client agrees to limit access to their computer network to those employees or consultants who require such access in order to use the computer network in furtherance of The Client business. The Client shall take all reasonable precautions to maintain the confidentiality of the computer network.

Joint management Responsibility

Both Creative Computer Solutions, Inc and The Client share responsibility for work management and oversight. Designated managers from both organizations will meet on a mutually defined regular basis to review business priorities and directions, key business milestones, work priorities, and shared work assignments. Designated managers from both Creative Computer Solutions, Inc and The Client will also be responsible for ensuring that high priority work is being addressed on a timely basis and that all key requirements are being met. Designated managers will be responsible for fully communicating issues and concerns and for ensuring that all team members are properly instructed on actions that need to be taken and corrections that need to be made. Designated managers will also be responsible for ensuring that agreed upon processes and work methods are being followed and that team members are appropriately aware of their responsibilities in carrying out their roles. Over and above these joint management responsibilities,

The Client has full and exclusive responsibility for understanding and ensuring compliance with any regulatory, legal or contractual obligations related to data held by The Client (or by Creative Computer Solutions, Inc on The Client behalf), information provided to customers and other third parties and safeguarding and security measures that may be required.



Creative Computer Solutions, Inc may participate in implementing needed systems services and functions, but The Client agrees that it shall be solely responsible for the final outcomes, actions taken and results produced.

Changes, Additions, Warranties, Stipulations or Lining Out

CCSI fees are based on an hourly rate and a combination of the time and labor required, the novelty and difficulty of the issues involved, the skill required to resolve the issues properly, the result obtained, and the fees customarily charged in our locality for similar services. The fees also depend on which member or employee of our company provides services on your behalf. The hourly rate is applied to time spent while working on any and all client projects; this may include project scope, network documentation, estimates, etc. Special Projects are presented to client as an estimate and do not constitute a fixed bid.

The warranty on all hardware, software, cabling, and peripherals supplied by CCSI, is provided by the manufacturer. Please refer to your account manager for specific warranty details.

Any changes, additions, stipulations or corrective lining out by The Client will not be binding to Creative Computer Solutions, Inc. until such additions, clauses or stipulations have been approved by means of a corrected contract or contract addendum prepared and signed by Creative Computer Solutions, Inc.

Indemnification

Creative Computer Solutions, Inc. agrees to indemnify and hold harmless The Client and its officers, board members, employees, their heirs, and agents, from any claim, liability, loss, costs or expense (including attorney fees and other costs and expenses of litigation through and including trial and appeals) caused by the alleged or actual negligent, reckless or intentional acts or omissions of Creative Computer Solutions, Inc., its employees or agents in rendering services pursuant to this contract.

The Client agrees to indemnify and hold harmless Creative Computer Solutions, Inc. and its officers, board members, employees, their heirs, and agents, from any claim, liability, loss, costs and expense (including attorney fees and other costs and expenses of litigation through and including trial and appeals) caused by the alleged or actual negligent, reckless or intentional acts or omissions of The Client its employees or agents in rendering services pursuant to this contract.

Alternative Dispute Resolution/Attorney Fees

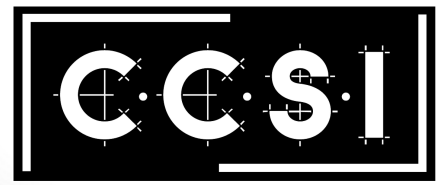
Any dispute over the interpretation or enforcement of this Agreement shall be submitted to the American Arbitration Association. The prevailing party in any dispute will be entitled to recover, in addition to all other damages provided by law, its reasonable attorney fees and costs incurred in submitting the matter to alternative dispute resolution, and if allowed, thereafter in any trial and on appeal.

Agreement in Entirety

This agreement contains the entire agreement between the parties. Any written or verbal promises, terms, conditions, or obligations other than those contained herein that are in any manner inconsistent or contradictory to those contained herein are null and void.

Withdrawal of Offer

This agreement / offer is considered null and void if not executed by both parties by within 30 days.



Authority to Execute Contract

It is acknowledged by the signature below that the signer has the authority from their respective organization to commit to this agreement, and sign this contract.

Creative Computer Solutions, Inc. looks forward to being of service to the staff of professionals at your company. We thank you for this opportunity and appreciate your consideration.

Signature

Date

City of Yacolt

First let me say thanks again for the opportunity to service you needs! Not enough businesses protect themselves with backups and Antivirus until they lost something so makes it a pleasure working with someone willing to be proactive.

While on site we assessed your current setup as follows:

I looked at 5 desktop in total 4 of which are in in use daily/weekly and around 5 years old Running Windows 7 these units are Dell Business line, I would recommend either replacing the Drives in these units or replacing the units all together within the next 2 years. Windows 7 has around 2 more years of Security and product support at that point you become vulnerable to the latest viruses/exploits. The 5th was a very outdated Vista system ((The Mayors) we recommend retiring this unit)

Some of the units had working Norton Antivirus on them and we would recommend switching this out for Eset Nod32.

Dawn's system was the only unit performing back-ups with Blaze not familiar with them or how great there service is we talked about Switching over to Mozy for Business as they have a 7 Year retention and Comply with all the newest HIPA policies

Prices for Items discussed which can be done at anytime:

2 or 3 Lenovo Thinkpad Laptops (Business Line), 15.6" Windows 10, i5 CPU, 500GB HDD \$800 each

We have units running \$650 with a much smaller CPU not gear towards business IMO

2x Eset AntiVirus 3 User 1Year Protection \$60 each

1x APC Battery Back 660VA \$95 each

Mozy Business Backup \$1 Per GB (GB Amount undetermined until data is cleaned up and combined)
Price break at +50GB goes to .60 Cents

Enterprise Grade External 2TB \$230 (unit is meant to be ran daily and house backups can be stored in a safe)

Google Apps for Business \$7/Mo Per User (Would allow everyone to use the Gmail portal to check mail, would also allow full cross platform Phone, Tablet, Computer in which Documents, Spreadsheets, Presentations could be shared and edited real time in the cloud, in addition 30GB of Google Drive Space per User allows them to Backup/Share from an easy to use interface.

TREASURERS REPORT

Fund Totals

Town Of Yacolt
MCAG #: 0254

04/01/2018 To: 04/30/2018

Time: 14:28:34 Date: 06/26/2018

Page: 1

Fund	Previous Balance	Revenue	Expenditures	Ending Balance	Claims Clearing	Payroll Clearing	Outstanding Deposits	Adjusted Ending Balance
001 Current Expense	755,330.79	123,790.54	19,881.66	859,239.67	59.96	517.14	-1,325.48	858,491.29
002 Current Expense Reserve Fund	115,332.54	0.00		115,332.54	0.00	0.00	0.00	115,332.54
101 Streets	-97,249.37	4,871.45	11,568.59	-103,946.51	0.00	4,882.94	0.00	-99,063.57
103 Cemetery	33,272.79	1,228.72	518.04	33,983.47	0.00	117.09	0.00	34,100.56
105 REET/Real Estate Excise Tax	135,252.68	2,024.55		137,277.23	0.00	66.95	0.00	137,344.18
114 Park Impact Fees	65,807.47	3,516.00		69,323.47	0.00	0.00	0.00	69,323.47
115 Transportation Impact Fees	77,189.14	4,222.35		81,411.49	0.00	0.00	0.00	81,411.49
403 Storm Water	54,423.97	0.00	2,478.80	51,945.17	0.00	2,454.36	0.00	54,399.53
	<u>1,139,360.01</u>	<u>139,653.61</u>	<u>34,447.09</u>	<u>1,244,566.53</u>	<u>59.96</u>	<u>8,038.48</u>	<u>-1,325.48</u>	<u>1,251,339.49</u>

TREASURERS REPORT

Account Totals

Town Of Yacolt
MCAG #: 0254

04/01/2018 To: 04/30/2018

Time: 14:28:34 Date: 06/26/2018
Page: 2

Cash Accounts	Beg Balance	Deposits	Withdrawals	Ending	Outstanding Rec	Outstanding Exp	Adj Balance
9 USBank 6765	698,099.93	140,673.66	35,467.14	803,306.45	-1,325.48	8,098.44	810,079.41
12 Investco MMA	325,927.54	0.00	0.00	325,927.54	0.00	0.00	325,927.54
13 Voya Financial	115,332.54	0.00	0.00	115,332.54	0.00	0.00	115,332.54
Total Cash:	1,139,360.01	140,673.66	35,467.14	1,244,566.53	-1,325.48	8,098.44	1,251,339.49
	1,139,360.01	140,673.66	35,467.14	1,244,566.53	-1,325.48	8,098.44	1,251,339.49

TREASURERS REPORT

Outstanding Vouchers

Town Of Yacolt
MCAG #: 0254

As Of: 04/30/2018 Date: 06/26/2018
Time: 14:28:34 Page: 3

Year	Trans#	Date	Type	Acct#	War#	Vendor	Amount	Memo
2017	1054	10/09/2017	Tr Rec	9		Permitting, Customer	199.50	
2017	1347	12/27/2017	Tr Rec	9		Permits - various	119.50	Todd Bladow - Plumbing Permit
2018	340	01/03/2018	Tr Rec	9			10.29	
2018	341	01/03/2018	Tr Rec	9			-20.58	
2018	211	03/06/2018	Tr Rec	9		Permitting, Customer	310.00	
2018	212	03/06/2018	Tr Rec	9		Permitting, Customer	1.00	
2018	232	03/13/2018	Tr Rec	9		Permitting, Customer	97.50	
2018	487	04/07/2018	Tr Rec	9		Burial Plot	20.00	Spring Cleanup
2018	330	04/10/2018	Tr Rec	9		Permitting, Customer	138.50	
2018	439	04/27/2018	Tr Rec	9		Burial Plot	4.00	Fax
2018	444	04/30/2018	Tr Rec	9		Carroll, Christopher	3.00	Puppy License
2018	445	04/30/2018	Tr Rec	9		Impact Automotive	45.00	Business License
2018	446	04/30/2018	Tr Rec	9		Pioneer Pest Management	45.00	Business License
2018	447	04/30/2018	Tr Rec	9		Coastal Pacific Excavating	45.00	Business License
2018	448	04/30/2018	Tr Rec	9		Rotschy, Inc.	250.00	Sponsorship Sidewalk Chalk Contest
2018	449	04/30/2018	Tr Rec	9		Sprint	35.59	Telephone Tax
2018	450	04/30/2018	Tr Rec	9		Granite Telecommunications, LLC	20.05	Telephone Tax
2018	451	04/30/2018	Tr Rec	9		Sprint	2.13	Telephone Tax
Receipts Outstanding:							1,325.48	
2018	196	03/05/2018	Payroll	9	EFT	AWC TRUST	3,912.58	02/28/2018 To 02/28/2018 - AWC Medical
2018	233	03/19/2018	Payroll	9	EFT	Department Of Retirement	112.79	Retirement Katie Retro Raise; Balance Pete Roberts
2018	377	01/18/2018	Payroll	9	0	AFLAC	66.95	
2018	408	04/30/2018	Payroll	9	EFT	AFLAC	44.07	04/01/2018 To 04/30/2018 - AFLAC- Accidental; 04/01/2018 To 04/30/2018 - Accident Rider
2018	338	01/03/2018	Claims	9	EFT		-10.29	
2018	339	01/03/2018	Claims	9	EFT		35.25	
2018	410	04/30/2018	Payroll	9	EFT	Department Of Retirement	2,084.78	04/01/2018 To 04/30/2018 - PERS 2
2018	154	02/20/2018	Payroll	9	EFT	AFLAC	149.11	Accidental
2018	136	01/29/2018	Payroll	9	EFT	AWC TRUST	1,604.03	01/01/2018 To 01/31/2018 - AWC Medical; 01/01/2018 To 01/31/2018 - Delta Dental; 01/01/2018 To 01/31/2018 - AWC Vision
2017	1308	12/18/2017	Claims	9	16412	WSAPT	35.00	Katie Younce Permit Technician Membership
2018	402	04/30/2018	Payroll	9	16530	Rhonda Rowe-Tice	64.17	
							8,098.44	

Fund	Claims	Payroll	Total
001 Current Expense	59.96	517.14	577.10

TREASURERS REPORT

Outstanding Vouchers

Town Of Yacolt
MCAG #: 0254

As Of: 04/30/2018 Date: 06/26/2018
Time: 14:28:34 Page: 4

Year	Trans#	Date	Type	Acct#	War#	Vendor	Amount	Memo	
Fund							Claims	Payroll	Total
101 Streets							0.00	4,882.94	4,882.94
103 Cemetery							0.00	117.09	117.09
105 REET/Real Estate Excise Tax							0.00	66.95	66.95
403 Storm Water							0.00	2,454.36	2,454.36
							59.96	8,038.48	8,098.44

TREASURERS REPORT

Signature Page

Town Of Yacolt
MCAG #: 0254

04/01/2018 To: 04/30/2018

Time: 14:28:34 Date: 06/26/2018
Page: 5

We the undersigned officers for the Town of Yacolt have reviewed the foregoing report and acknowledge that to the best of our knowledge this report is accurate and true:

Signed: _____ Signed: _____
Mayor / Date Clerk / Date

TREASURERS REPORT

Fund Totals

Town Of Yacolt
MCAG #: 0254

05/01/2018 To: 05/31/2018

Time: 14:34:51 Date: 06/26/2018

Page: 1

Fund	Previous Balance	Revenue	Expenditures	Ending Balance	Claims Clearing	Payroll Clearing	Outstanding Deposits	Adjusted Ending Balance
001 Current Expense	859,239.67	38,773.95	23,907.46	874,106.16	317.00	954.82	-1,185.71	874,192.27
002 Current Expense Reserve Fund	115,332.54	0.00		115,332.54	0.00	0.00	0.00	115,332.54
101 Streets	-103,946.51	3,050.74	14,658.11	-115,553.88	216.58	6,345.94	0.00	-108,991.36
103 Cemetery	33,983.47	500.00	117.66	34,365.81	0.00	131.30	0.00	34,497.11
105 REET/Real Estate Excise Tax	137,277.23	3,625.99		140,903.22	0.00	66.95	0.00	140,970.17
114 Park Impact Fees	69,323.47	0.00		69,323.47	0.00	0.00	0.00	69,323.47
115 Transportation Impact Fees	81,411.49	0.00		81,411.49	0.00	0.00	0.00	81,411.49
403 Storm Water	51,945.17	0.00	2,243.45	49,701.72	0.00	2,738.31	0.00	52,440.03
	<u>1,244,566.53</u>	<u>45,950.68</u>	<u>40,926.68</u>	<u>1,249,590.53</u>	<u>533.58</u>	<u>10,237.32</u>	<u>-1,185.71</u>	<u>1,259,175.72</u>

TREASURERS REPORT

Account Totals

Town Of Yacolt
MCAG #: 0254

05/01/2018 To: 05/31/2018

Time: 14:34:51 Date: 06/26/2018

Page: 2

Cash Accounts	Beg Balance	Deposits	Withdrawals	Ending	Outstanding Rec	Outstanding Exp	Adj Balance
9 USBank 6765	803,306.45	45,950.68	40,926.68	808,330.45	-1,185.71	10,770.90	817,915.64
12 Investco MMA	325,927.54	0.00	0.00	325,927.54	0.00	0.00	325,927.54
13 Voya Financial	115,332.54	0.00	0.00	115,332.54	0.00	0.00	115,332.54
Total Cash:	1,244,566.53	45,950.68	40,926.68	1,249,590.53	-1,185.71	10,770.90	1,259,175.72
	1,244,566.53	45,950.68	40,926.68	1,249,590.53	-1,185.71	10,770.90	1,259,175.72

TREASURERS REPORT

Outstanding Vouchers

Town Of Yacolt
MCAG #: 0254

As Of: 05/31/2018 Date: 06/26/2018
Time: 14:34:51 Page: 3

Year	Trans#	Date	Type	Acct#	War#	Vendor	Amount	Memo
2017	1054	10/09/2017	Tr Rec	9		Permitting, Customer	199.50	
2017	1347	12/27/2017	Tr Rec	9		Permits - various	119.50	Todd Bladow - Plumbing Permit
2018	340	01/03/2018	Tr Rec	9			10.29	
2018	341	01/03/2018	Tr Rec	9			-20.58	
2018	211	03/06/2018	Tr Rec	9		Permitting, Customer	310.00	
2018	212	03/06/2018	Tr Rec	9		Permitting, Customer	1.00	
2018	232	03/13/2018	Tr Rec	9		Permitting, Customer	97.50	
2018	487	04/07/2018	Tr Rec	9		Burial Plot	20.00	Spring Cleanup
2018	330	04/10/2018	Tr Rec	9		Permitting, Customer	138.50	
2018	530	05/23/2018	Tr Rec	9		Permitting, Customer	65.00	
2018	583	05/31/2018	Tr Rec	9		North Fork Drywall	45.00	Business License
2018	584	05/31/2018	Tr Rec	9		Fort Vancouver Regional Library	200.00	Library Lease
Receipts Outstanding:							1,185.71	
2018	338	01/03/2018	Claims	9	EFT		-10.29	
2018	410	04/30/2018	Payroll	9	EFT	Department Of Retirement	2,084.78	04/01/2018 To 04/30/2018 - PERS 2
2018	154	02/20/2018	Payroll	9	EFT	AFLAC	149.11	Accidental
2018	196	03/05/2018	Payroll	9	EFT	AWC TRUST	3,912.58	02/28/2018 To 02/28/2018 - AWC Medical
2018	377	01/18/2018	Payroll	9	0	AFLAC	66.95	
2018	339	01/03/2018	Claims	9	EFT		35.25	
2018	547	05/29/2018	Payroll	9	EFT	Department Of Retirement	2,102.58	05/01/2018 To 05/31/2018 - PERS 2
2018	136	01/29/2018	Payroll	9	EFT	AWC TRUST	1,604.03	01/01/2018 To 01/31/2018 - AWC Medical; 01/01/2018 To 01/31/2018 - Delta Dental; 01/01/2018 To 01/31/2018 - AWC Vision
2018	233	03/19/2018	Payroll	9	EFT	Department Of Retirement	112.79	Retirement Katie Retro Raise; Balance Pete Roberts
2018	545	05/29/2018	Payroll	9	EFT	AFLAC	44.07	05/01/2018 To 05/31/2018 - AFLAC- Accidental; 05/01/2018 To 05/31/2018 - Accident Rider
2018	507	05/21/2018	Claims	9	16550	Larch Correctional Center	216.58	
2018	510	05/21/2018	Claims	9	16553	The Reflector	30.00	
2018	511	05/21/2018	Claims	9	16554	U. S. Bank Corporate Payment System	262.04	
2018	543	05/31/2018	Payroll	9	16555	Rhonda Rowe-Tice	160.43	
							10,770.90	

Fund	Claims	Payroll	Total
001 Current Expense	317.00	954.82	1,271.82
101 Streets	216.58	6,345.94	6,562.52
103 Cemetery	0.00	131.30	131.30
105 REET/Real Estate Excise Tax	0.00	66.95	66.95

TREASURERS REPORT

Outstanding Vouchers

Town Of Yacolt
MCAG #: 0254

As Of: 05/31/2018 Date: 06/26/2018
Time: 14:34:51 Page: 4

Year	Trans#	Date	Type	Acct#	War#	Vendor	Amount	Memo	
Fund							Claims	Payroll	Total
403 Storm Water							0.00	2,738.31	2,738.31
							533.58	10,237.32	10,770.90

TREASURERS REPORT

Signature Page

Town Of Yacolt
MCAG #: 0254

05/01/2018 To: 05/31/2018

Time: 14:34:51 Date: 06/26/2018
Page: 5

We the undersigned officers for the Town of Yacolt have reviewed the foregoing report and acknowledge that to the best of our knowledge this report is accurate and true:

Signed: _____ Signed: _____
Mayor / Date Clerk / Date