

Bids for Implement the Internet Server Firewall License Renewal

CPD15/1057/2021

Bid Closing Date and Time: 22 / 07 / 2021 at 10.00 am

Bid Opening Date and Time: 22 / 07 / 2021 at 10.00 am

PART I

(For office use only)

Name of the Firm: -

Receipt No.: -.....

.....

Issuing Officer

Date: -.....

PART II

(To be filled by the Bidder)

1. Name of the Bidder: -.....

2. Business Address: -.....

.....

.....

3. Telephone Numbers: -.....

4. Email Address: -

5. Business Registration No: -.....

6. VAT Registration No: -

Bank Guarantee No: -.....

Bank: -.....

Bank Guarantee Amount: -.....

Price Schedule

	Description	QTY	Total Annual Charges (Without Tax)	08% Vat	Total Annual Charges (With Tax)	Total Charges for Three Years (With Tax)
01	Firewall HW Appliance	02				
02	Full Protection Licenses	02				
03	Email Protection	02				
04	Webserver Protection	02				

I agree that the price given in this bid is valid for acceptance for a period of one year from the date of closing of Bids and the quoted price will be firm and not subject to adjustment not can it be withdrawn after closing of the bids.

WITNESSES

.....
SIGNATURE OF BIDDER
AND SEAL OF THE FIRM.

NAME IN BLOCK CAPITALS:-.....

ADDRESS: -

.....

(1). Signature :

Name in Block Capitals :

Address :

(2). Signature :

Name in Block Capitals :

Address

Colombo Municipal Council

Bids for Implement the Internet Server Firewall License Renewal

BID CONDITIONS AND INSTRUCTIONS TO BIDDERS

SCOPE OF THE BID.

Bidders are hereby invited by the Municipal Commissioner, Colombo Municipal Council to supply, install, configure and maintain a Firewall system on the Internet server. The system is implemented at Colombo Municipal Council, Town Hall, Colombo 07.

Please Contact on Telephone **077 359 5801** - (System Consultant/ CMC) before visiting the Colombo Municipal Council Premises.

Bidders **should be eligible as detailed in the Conditions and Specifications** for acceptance for evaluation of their bids.

1.0 RECEIPT OF BIDDERS

A. General

1.1 The Purchaser is: Colombo Municipal Council

1.2 The name of the NCB is of **Bids for Implement the Internet Server Firewall License Renewal**

1.3 The source of funding is: CMC Funds

B. Contents of Bidding Documents

1.4 For **Clarification of bid purposes** only, the Purchaser's address is:

Attention: Chief Accountant (Procurement)

Address: Central Procurement Department, Colombo Municipal Council

Telephone: 2686389

Facsimile number: 2662329

Electronic mail address: caccproc@colombo.mc.gov.lk

1.5 The Bidder shall submit the following additional documents: [insert list of documents, if any]

1.5.1. Full document of Bidders Company Registration/Business Registration

1.5.2. Details of performance evidence for past three years. (Awarding letters, Purchase orders & performance letters etc.)

1.5.3. Copy of VAT Registration letter if Vat registered.

1.5.4. In case the relevant bid value of the items for which expected to submit the bidding documents exceed Rupees five(5)million, the registration certificate obtained from the public Contracts Registrar (PCR)Colombo by the representative agent, Sub agent or nominee/nominated representative for and on behalf of the Bidder should be submitted.

2.0 OPENING OF BIDDERS

C. Preparation of Bids

2.1 The bid shall be valid until 6 months.

2.2 (a) Bid shall include a Bid Security (issued by bank) included in Section IV Bidding Forms;

Bid Guarantee obtained in favor of the Municipal Commissioner to the value of Rs.100,000.00 (Rupees One Hundred Thousand only) valid for 180 days (One hundred and Eighty days) from the closing date of bids should be provided along with the bid. Bank Guarantee should be obtained only from a recognized Bank accepted by the Central Bank of Sri Lanka under Banking Act No: 30 of 1988.

2.3 Any bids not accompanied by bid Security Guaranty pursuant to clause 3.1 will be rejected and no further consideration will be given to such Bids.

2.4 After the award has been finalized the bid Security Guaranty will be released to the respective bidders with the exception of the successful Bids. The bid Security Guaranty of the successful bidders will be released after furnishing of required Performance Guaranty and signing of Contract Agreement by the Bidder.

2.5 The amount of the Bid Security shall be: **Rs.100,000.00**

2.6 The validity period of the bid security shall be until:

From **2021.07.22** to **2022.01.21** (One Hundred and Eighty days)

D. Submission and Opening of Bids

2.7 The inner and outer envelopes shall bear the following identification marks: Bids for Implement the Internet Server Firewall License Renewal
CPD 15/ 1057 /2021

2.8 For bid submission purposes, the Purchaser's address is:

Attention: Municipal Commissioner

Address: Colombo Municipal Council, Town hall, Colombo 07

The deadline for the submission of bids is:

Date 2021.07.22

Time: 10.00 am

2.9 The bid opening shall take place at: Colombo Municipal Council

2.10 Address: Municipal Secretary's Department, Colombo Municipal Council, Town Hall, Colombo 07.

Date: 2021.07.22

Time: 10.00 a.m

2.11 Thereafter Both ORIGINAL and DUPLICATE should be enclosed to one envelop and Sealed AND mark the Name of bidding item to be supplied on top left hand corner and Closing Date and Address to Municipal Commissioner, Colombo Municipal Council, Town Hall, Colombo 07. BIDDER'S Name and Address should be written on each envelope.

2.12 The duly perfected bids Should be deposited in the (Bid Box) kept in the Municipal Secretary's Department, Town Hall, Colombo 07, before closing as per time and date, published in the press Notice

2.13 BIDDERS or their authorized representatives are allowed to be present at the time of opening of the bids.

3.0 BID SECURITY GUARANTEE

3.5 The successful bidder on receipt of the letter of acceptance of bid should be submitted within seven (07) working days submit the Performance Guaranty and sign the Contract Agreement with the Colombo Municipal Council within 21 days.

3.6 In the event of successful bidder failing to provide performance Guaranty and to sign the contract agreement within the stipulated time period referred to in paragraph 3.5 above, the bidder is liable to forfeit the bid Security Guaranty or undergo any other penalty imposed by the Council or our firm, its affiliates or subsidiaries—including any subcontractors or suppliers for any part of the contract—has not been declared blacklisted by the National Procurement Agency or liable to accept.

4.0 MINIMUM VALIDITY PERIOD OF OFFERS

4.1 All offers shall be valid for a minimum period of 180 (Hundred Eighty) calendar days from the date of closing of the bid.

4.2 All prices quoted shall be firm and shall not be subject to any price variation within the validity period of offer specified above.

05. POWER OF THE COUNCIL TO ACCEPT OR REJECT THE OFFERS

The Council reserves the right to reject any or all bids or any portion of the bid without adducing any reason. The Council may award the contract for any particular set of items at the quoted maintenance charges for each item. The Council is not liable and not bound to accept the lowest price bid(s).

06. COMPOSITION AND EVALUATION OF BIDS

- 6.1 Bidders will be qualified on the information regarding their corporate and staff strength, ability to perform contracts of this nature, and satisfactory performance in maintenance of systems comparable to that of CMC. The following will be examined as stated and provided by the Bidders, in the form for Qualification, Schedule A (1). (See Clause 26.1).
- a) Computer systems comparable to that of Buyer, maintained by the Bidder.
 - b) Qualifications and experience of the Bidder's relevant computer system maintenance staff.
 - c) Availability of and access to spare parts and diagnostic and maintenance tools, instruments and techniques specific to the equipment to be maintained.
 - d) Reference sites.
- 6.2 The offers will be compared on the following basis and the most responsive bid will be selected (See Clause 26.2).
- a) Compliance with the bidding conditions.
 - b) Bidder's qualifications and ability to commence the required maintenance work quickly.
 - c) Manufacture authorization.

07. WARRANTY

- 7.1 The contractor guarantees to the Council and the Commissioner, Colombo Municipal Council, that maintenance under the contract will comply strictly with the requirements of the contract.
- 7.2 The contractor shall further guarantee that no equipment, materials, software (programs) or data of the CMC or at CMC will be damaged or lost by any actions or negligence of the contractor's staff.
- 7.3 The contractor guarantees that all software and data of Buyer will be treated in the strictest confidence.
- 7.4 The contractor guarantees that his staff, particularly those assigned for CMC work, are fully trustworthy.
- 7.5 The maintenance agreement should be entered into with the Colombo Municipal Council.

08. SCHEDULE OF PRICES

- 8.1 Bidders shall complete and sign the prescribed form of schedule of prices. The charges quoted should be for comprehensive maintenance services including parts and labor. If any parts or components or user-replaceable parts of equipment are not covered by the maintenance services those must be clearly stated in the bid. Net price should cover travel and any other expenses incurred on maintenance work. Failure to provide the net price may result in the bid being considered as a non-responsive bid. The price schedule should be submitted with the bid.
- 8.2 Bidder must **quote annual charges for Bids for Implement the Internet Server Firewall License Renewal** including all equipment's and software **attached inside**.
- 8.3 The price quoted should be written clearly in ink or typewritten and must be in figures and repeated in words. If there is a discrepancy between the prices stated in figures and words, the prices stated in words will be taken as correct.
- 8.4 Any alteration in the offers should be initialed by the bidder. Failure to do so will result in the offer being treated as informal and it will be rejected.

09. PROOF OF ABILITY

- 9.1 Bidders should be prepared to produce documentary evidence of ability to carry out the maintenance for which bids are invited, if called upon to do so, before bid is awarded to them.
- 9.2 Bidders should be prepared to disclose reference sites, the contact persons and other information of their client installations, which will be kept confidential by the Council.
- 9.3 Bidders should be prepared to produce copies or originals of Certificates and agreements pertaining to the bid, which will be kept confidential by the Council.

10. ELIGIBLE BID/BIDDER

- 10.1 The invitation for Bids is open to all reputed computer system maintenance parties with at least five (5) years of experience. The experience of the bidder and his staff must be clearly stated in the bid.
- 10.2 The bidder must have stocks of and proven access to spare parts for server systems and other equipment for which maintenance is required under this bid. Bidder must be prepared for inspection of such stocks by Buyer, during evaluation of bids.

11. PERFORMANCE GUARANTY

- 11.1 A sum equivalent to ten percent (10%) of the total value of the contract by Bid Bond is required as a Performance guaranty for the due fulfillment of the contract by the successful Bidder. If the Commissioner, Colombo Municipal Council is of opinion that the performance of the successful Bidder is unsatisfactory and that there is a breach of the stipulated conditions of the agreement, the Performance guaranty is liable to be forfeited and the contract terminated.
- 11.2 The Performance guaranty will be returned to the supplier at the end of the contract period if performance is satisfactory.

12. NOTIFICATION

- 12.1 Notice of acceptance of the bid will be sent to the selected bidder by registered post to the address given by him/them in the bid.

13. CONTRACT NOT TO BE SUB-LET

- 13.1 The Contractor shall not assign or sub-let the contract or any part thereof or any benefit or interest therein to any third party without the prior written consent of the Commissioner, Colombo Municipal Council. The contractor shall not issue a power of Attorney to any person whose name is on the list of defaulting contractors for carrying on work under the contract.

14. SIGNING OF THE CONTRACT AGREEMENT

- 14.1 The successful bidder should enter into a contract agreement within the stipulated time as in clause 3.5 with the Colombo Municipal Council. The successful bidder must be prepared if so required by the on acceptance of bid to provide two good and trustworthy sureties acceptable to the Commissioner to guarantee the due fulfillment of the contract and the punctual performance of the agreement.
- 14.2 Contract will be signed for 2 years soon after the signing the contract.

15. APPLICABLE LAW

- 15.1 The bids and any contracts resulting there from shall be governed and abide by the laws of Democratic Socialist Republic of Sri Lanka.

16. FORCE MAJEURE

- 16.1 Neither party will be held responsible for failing in the execution of its contractual obligations in case their execution is delayed or hampered by force majeure events.
- 16.2 In the execution of the contract the term FORCE MAJEURE includes but is not restricted to acts of god, acts of civil insurrection, fires, floods, epidemics, strikes, freight embargoes and explosions.
- 16.3 If the contractor notifies the Commissioner in writing of the cause of such failure within 30 days from the beginning thereof, he may grant an extension of the delivery time when, in his judgment the facts justify such an extension. His findings shall be conclusive, subject only to the contractor's right of appeal under the arbitration clause of the contract.

17. MAINTENANCE RESPONSE

The time duration for maintenance/repair will be agreed upon by the contractor and the Buyer, as stipulated in the Specifications.

- 17.1 Should be installed / configured within the said and agreed time period.
- 17.2 If any issue with the installed firewall system, should be attended within two (02) Hrs including holidays / weekends / out of office hours.
- 17.3 Should be able to make the system up and running within four (04) Hrs after the breakdown call is logged.
- 17.4 Should be able to create and apply “rules” as per CMC requirement.
- 17.5 If any assigned rule to be changed or new rule to be implemented, should be attended only with an official request from the IT Div. and should be attended within two (02) Hr.
- 17.6 If removing existing firewall from the site for repairs an On –loan should be provided to continue operations uninterrupted.
- 17.7 Maintain records of preventive maintenance and repairs carried out should be handed over to the IT Div., CMC, so that recurring defects and patterns of defects can be identified for preventive measures.
- 17.8 Take measures to ensure security and confidentiality of all data, programs and system of Buyer.

18. MAINTENANCE TYPES

18.1 Maintenance includes preventive maintenance and repair of defects and replacement of defective components and re-commissioning of equipment and system as relevant.

19. MODE OF PAYMENT

19.1 Full Payment after the installation and commissioning.

20. TERMINATION OF THE CONTRACT

20.1 The Commissioner, Colombo Municipal Council may without prejudice to any other remedy for breach of contract, by written notice of default sent to the contractor, terminate the contract in whole or in part:

a) If the contractor fails to provide the services as required and within the time agreed, or any extension thereof granted by the Commissioner, Colombo Municipal Council.

b) If the contractor fails to perform any other obligation(s) under the contract

and

If the contractor in either of the above circumstances, does not respond within a period of two (2) calendar days after receipt of the notice of default from the Commissioner, CMC, specifying the nature of the default(s).

21. TIME EXTENSION FOR THE CONTRACTOR'S PERFORMANCE

21.1 Maintenance services shall be provided by the contractor in accordance with the time durations agreed upon as stated in clause 17.

21.2 The contractor may claim extension of the time durations in case of Force Majeure events or, reasons related to nature of computer system, or the Buyer's business operations.

21.3 The contractor shall not be entitled to an extension of time for completion of tasks unless the contractor at the time of such circumstances arising (immediately) has notified the Commissioner, Colombo Municipal Council, in writing, of the delay that it may claim as caused by circumstances pursuant to clause 20 above, and upon request of the Commissioner, Colombo Municipal Council, the contractor shall substantiate that the delay is due to the circumstances referred to by the contractor.

22. GENERAL PROVISION

- 22.1 The contractor shall indemnify the Democratic Socialist Republic of Sri Lanka against any claim by or in respect of any employee of the contractor under the Workmen's Compensation Ordinance, No. 19 of 1934 or any statutory amendments, modifications or extensions thereof.
- 22.2 Contractors shall acquaint themselves fully with the conditions of the contract. No plea for lack of information will be entertained at any time.
- 22.3 Commissioner, Colombo Municipal Council, notwithstanding this agreement shall be at liberty to make other arrangements for maintenance services, should it appear advisable to him to do so, and in such an event the contractor shall not be entitled to claim any damages against the Colombo Municipal Council.

23. DECLARATION OF THE DIRECTORS AND FINANCIAL DETAILS

- 23.1 Bidders should declare in the case of Private Company the names of all Directors and Shareholders of the Company. If the company is a Public Company, the names of Directors should be declared.

24. DETAILS TO ACCOMPANY THE BID

- 24.1 The following details and documents should accompany the bid.
- a) The Qualification Form completed and duly signed together with relevant documents - Schedule A (i)
 - b) Bid Security Guarantee - Schedule A (ii)
 - c) Documents as proof of ability vide clause 9.0.
 - d) Customer and systems list.
 - e) Bid Decrement duly signed - Schedule B (i).
 - f) General Conditions of the bid duly signed.
 - g) Schedule of Prices duly signed - Schedule B (ii)
 - h) Staff details and spare parts availability. Schedule B (iii)

The above documents and any other deemed necessary, shall be enclosed in an envelope or wrapper and sealed, in duplicate, stating the name and address of the Bidder and stating "Bids for **Implement the Internet Server Firewall License Renewal**" on top left corner of the envelope or wrapping.

25. FURTHER INFORMATION

25.1 Further information can be obtained from the Commissioner, Colombo Municipal Council, Town Hall, Colombo 3, on any working day between hours of 10.00 a.m. to 2.30 p.m. until the close of Bid.

I/We agree to abide by the above conditions of bids.

.....
Signature of Bidder
& Designation Company Seal

Date:

Specimen Form for Qualification of Bidder

Bids for Implement the Internet Server Firewall License Renewal

Instruction to Bidders

1. The system for which maintenance services are requested by this bid is utilized for vital business activities of the Buyer. The contractor should be able to maintain the computer system for flawless operation.
2. The details requested in this Specimen Form should be completed with great care providing all genuine information which could be verified from other sources.

Qualification Details

1. Name of Bidder:
- Name of Company:
- Nature of Organization:

(State whether Individual, Corporation, Partnership or other)

Office Address:
.....
.....

Telephone:

Fax:

2. Name of Directors:
.....
.....
.....

3. Corporate standing /relationship with equipment manufacturers/principals relevant for the services offered.

.....
.....
.....
.....
.....

4. Date and Number of Business Registration/ Company Registration:.....

(Copy of the registration should be enclosed)

5. What was the first client's computer network system maintained by bidder:

Client:

Configuration:

Duration: Start date: End date:

.....

6.1 Please give a list of Equipment maintenance assignments completed by the bidder and those in progress, as evidence of required experience. This information will be used to assess Bidder's competence to maintain the specific equipment for which maintenance services are offered.

Client Description of Equipment/Systems Dates (from-to)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

6.2 Staff in bidder's employment for Computer Equipment/System maintenance.

.....
.....
.....
.....
.....
.....
.....
.....

6.3 Reference Sites

Please give three (3) reference sites in the public sector, where computer equipment and network systems are maintained by bidder. If the number of public sector reference sites is less than three, then give reference sites in the private sector too.

Client	Configuration	Duration of Maintenance	Contact Person
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

7. Financial Statements of Bidder.

Copy of Auditioned Statements Accounts for last two financial years should submitted. Financial Statements shall be certified by a chartered Accountant / Audit Firm.

I/We certify that the details given above (1 to 7) are true and accurate.

I/We attach hereto the following documents as part of my/our bid.

- a) Bid Security
- b) Bid Decrement
- b) Documents as proof of ability vide clause 9.0.
- c) List of customers.

Address:

Telephone:

Fax:

Signature of Bidder:

Name of Bidder:

Designation of Bidder:

Company Seal:

Date:

Bids for Implement the Internet Server Firewall License Renewal

ACCEPTABLE FORMAT FOR PERFORMANCE GUARANTEE

..... (Issuing Agency’s Name, and Address of Branch or Office).....

Beneficiary :.....(Name and Address of Employer).....

Date:

PERFORMANCE GUARANTEE NO

We have been informed that (Name of Supplier) (Hereinafter called “the Supplier”) has entered into bid/quotation No..... (reference number of the bid/quotation) dated.....with you, for the(Insert “Supply”) of (name of supply and brief description of supply) (hereinafter called “the supply”)

Furthermore, we understand that, according to the conditions of the supply a performance guarantee is required.

At the request of the supplier, We (name of Agency) here by irrevocably undertake to pay you any sum or sums not exceeding in total an amount of (Amount in figures)(.....) (amount in Words), Such sum being payable in the types and proportions of currencies in which the supply price is payable, up on receipt by us of yours first demand in writing accompanied by a written statement starting that the Supplier is in breach of its obligation(s) under the supply, without your needing to prove or to show grounds for your demand or the sum specified therein.

This guarantee shall expire, no later than the Day of20..... (Insert date, 28 Days beyond the scheduled Supply completion date) and any demand for payment under it must be received by us at this office on or before that date.

.....
[Signature(s)]

Schedule B(i)

Bids for Implement the Internet Server Firewall License Renewal

SPECIMEN BID FORM

Colombo Municipal Council
Town Hall
Colombo 07.

Bids for Implement the Internet Server Firewall License Renewal

1. I/We, the undersigned, having read and fully acquainted myself / ourselves with the contents of the "Information and Instructions to Bidders and Terms and Conditions of Bid" pertaining to the above Bid, along with Forms and Schedules thereto, do hereby undertake to provide maintenance services referred to therein, in accordance with the aforesaid Instructions. Terms and conditions, for a total Bid Price of Sri Lanka Rupees (SLRs) The make up of the aforesaid Total Bid Price is given in the accompanying Price Schedules.
2. I/We confirm that this offer shall be open for acceptance until..... and that it will not be withdrawn or revoked prior to that date.
3. I/We attach hereto the following documents as part of my/our Bid:
 - (a) Bid Documents duly signed
 - (b) General Conditions of the Bid duly signed
 - (c) Special Conditions and Bid Specifications
 - (d) Offered Products and Services with their specifications
 - (e) Schedule of Prices duly signed
 - (f) Declaration of Directors vides clause 25.0, and Qualification Form.
 - (g) Warranty vide clause 7.0
 - (h) Test Reports and any other relevant documents or details.
4. I/We understand that The Colombo Municipal Council is not bound to accept the lowest Bid and that The Colombo Municipal Council has the right to reject any or all Bids or to accept any part of a Bid.
5. I/We undertake to adhere to the Delivery Schedules given in the respective Price Schedule.
6. My/Our Bank Reference is as follows:
.....
.....
7. My/Our address for the purpose of this Bid and the Contract, if awarded, is as follows:

Address:
.....
Telephone:
Fax:
Signature of Bidder:
Name of Bidder:
Designation of Bidder:
Company Seal:
Date:

Schedule B (ii)

Bids for Implement the Internet Server Firewall License Renewal

**Tender Specification of
Next Generation Firewall / Cybersecurity Gateway Solution**

Technical Specifications		Comply / Non Comply	Compliance Yes / No	Remarks
Model :		Please specify		
Country of Origin :		Please specify		
Number of device required		02		As per the existing server configurations, 2 are needed one for front end and one for back end.
01	General Configuration			
1.10	Firewall throughput - 40 Gbps	Comply		
1.20	IPS throughput- 13 Gbps	Comply		
1.30	Threat Protection throughput - 2.5 Gbps	Comply		
1.40	Concurrent connections - 13,500,000	Comply		
1.50	New connections/sec - 250,000	Comply		
1.60	SSL/TLS Inspection throughput - 3 Gbps	Comply		
02	Physical interfaces			
2.10	Integrated min. 240 GB SATA-III SSD for Local quarantine / logs	Comply		
2.20	Minimum 8 x GE copper Ethernet Interfaces	Comply		
2.30	2 x SFP fiber Interface Ports	Comply		
2.40	2 x SFP+ 10 GbE fiber Interface Ports	Comply		
2.50	One bypass port pairs	Comply		
2.60	Minimum one expansion slots	Comply		
2.70	Multi-function LCD Display	Comply		
03	General Management			
3.1	Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators	Comply		

3.2	Two-factor authentication (One-time-password) support for administrator access, user portal, IPsec and SSL VPN	Comply		
3.3	Advanced trouble-shooting tools in GUI (e.g. Packet Capture)	Comply		
3.4	High Availability (HA) support clustering two devices in active-passive mode.	Comply		
3.5	Full command-line-interface (CLI) accessible from GUI	Comply		
3.6	Role-based administration	Comply		
3.7	Automated firmware update notification with easy automated update process and roll-back features	Comply		
3.8	Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers	Comply		
3.9	Jumbo Frame Support	Comply		
3.10	Self-service user portal	Comply		
3.11	Configuration change tracking	Comply		
3.12	Flexible device access control for services by zones	Comply		
3.13	Email or SNMP trap notification options	Comply		
3.14	SNMPv3 and Net flow support	Comply		
3.15	Centralized management support via cloud base platform	Comply		
3.16	Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly	Comply		
3.17	API for 3rd party integration	Comply		
3.18	Interface renaming	Comply		
3.19	Remote access option for Vendor Support	Comply		
3.20	Cloud-based license management via Cloud account	Comply		
04	Firewall, Networking & Routing			
4.1	Stateful deep packet inspection firewall	Comply		
4.2	Network Flow acceleration for trusted traffic	Comply		
4.3	User, group, time, or network based policies	Comply		
4.4	Access time polices per user/group	Comply		
4.5	Enforce policy across zones, networks, or by service type	Comply		

4.6	Zone isolation and zone-based policy support	Comply		
4.7	Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi	Comply		
4.8	Custom zones on LAN or DMZ	Comply		
4.9	Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule	Comply		
4.10	Flood protection: DoS, DDoS and portscan blocking	Comply		
4.11	Country blocking by geo-IP	Comply		
4.12	Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF)	Comply		
4.13	Upstream proxy support	Comply		
4.14	Protocol independent multicast routing with IGMP snooping	Comply		
4.15	Bridging with STP support and ARP broadcast forwarding	Comply		
4.16	VLAN DHCP support and tagging	Comply		
4.17	VLAN bridge support	Comply		
4.18	WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules	Comply		
4.19	Wireless WAN support (n/a in virtual deployments)	Comply		
4.20	802.3ad interface link aggregation	Comply		
4.21	Full configuration of DNS, DHCP and NTP	Comply		
4.22	Dynamic DNS (DDNS)	Comply		
4.23	IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec	Comply		
05	Base Traffic Shaping & Quotas			
5.1	Flexible network or user based traffic shaping (QoS)	Comply		
5.2	Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical	Comply		
5.3	Real-time VoIP optimization	Comply		
5.4	DSCP marking	Comply		
06	Authentication			
6.1	Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+	Comply		

6.2	Server authentication agents for Active Directory SSO, STAS, SATC	Comply		
6.3	Single sign-on: Active directory, eDirectory, RADIUS Accounting	Comply		
6.4	Client authentication agents for Windows, Mac OS X, Linux 32/64	Comply		
6.5	Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos	Comply		
6.6	Browser Captive Portal	Comply		
6.7	Authentication certificates for iOS and Android	Comply		
6.8	Authentication services for IPsec, SSL, L2TP, PPTP	Comply		
6.9	Google Chromebook authentication support for environments with Active Directory and Google G Suite	Comply		
6.10	API-based authentication	Comply		
07	User Self-Service Portal			
7.1	Download SSL remote access client (Windows) and configuration files (other OS)	Comply		
7.2	Hotspot access information	Comply		
7.3	Change user name and password	Comply		
7.4	View personal internet usage	Comply		
08	Base VPN Options			
8.1	Site-to-site VPN: SSL, IPsec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key	Comply		
8.2	L2TP and PPTP	Comply		
8.3	Route-based VPN	Comply		
8.4	Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Android VPN client support	Comply		
8.5	IKEv2 Support	Comply		
8.6	SSL client for Windows and configuration download via user portal	Comply		
09	IPsec VPN Client			
9.1	Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH	Comply		
9.2	Intelligent split-tunneling for optimum traffic routing	Comply		
9.3	NAT-traversal support	Comply		

9.4	Client-monitor for graphical overview of connection status	Comply		
9.5	Mac and Windows Support	Comply		
10	Intrusion Prevention (IPS)			
10.1	High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	Comply		
10.2	Thousands of signatures	Comply		
10.3	Granular category selection	Comply		
10.4	Support for custom IPS signatures	Comply		
10.5	IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added	Comply		
11	ATP			
11.1	Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	Comply		
12	Clientless VPN			
12.1	Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC	Comply		
13	Web and Network Protection and Control			
13.1	Fully transparent proxy for anti-malware and web-filtering	Comply		
13.2	Enhanced Advanced Threat Protection	Comply		
13.3	URL Filter database with millions of sites with appropriate categories	Comply		
13.4	Surfing quota time policies per user/group	Comply		
13.5	Access time polices per user/group	Comply		
13.6	Malware scanning: block all forms of viruses, web malware, Trojans and spyware on HTTP/S, FTP and web-based email	Comply		
13.7	Advanced web malware protection with JavaScript emulation	Comply		
13.8	Live Protection real-time in-the-cloud lookups for the latest threat intelligence	Comply		
13.9	Second independent malware detection engine for dual-scanning	Comply		
13.10	Real-time or batch mode scanning	Comply		

13.11	HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions	Comply		
13.12	SSL protocol tunneling detection and enforcement	Comply		
13.13	Certificate validation	Comply		
13.14	High performance web content caching	Comply		
13.15	File type filtering by mime-type, extension and active content types (e.g. ActiveX, applets, cookies, etc.)	Comply		
13.16	YouTube for Schools enforcement per policy (user/group)	Comply		
13.17	Safe Search enforcement (DNS-based) for major search engines per policy (user/group)	Comply		
13.18	Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists	Comply		
13.19	Block Potentially Unwanted Applications (PUAs)	Comply		
13.20	Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users	Comply		
13.21	User/Group policy enforcement on Google Chromebooks	Comply		
13.22	TLS 1.3 inspection with pre-packaged exceptions	Comply		
14	Cloud Application Visibility			
14.1	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated	Comply		
14.2	Discover Shadow IT at a glance	Comply		
14.3	Drill down to obtain details on users, traffic, and data	Comply		
14.4	One-click access to traffic shaping policies	Comply		
14.5	Filter cloud application usage by category or volume	Comply		

14.6	Detailed customizable cloud application usage report for full historical reporting	Comply		
15	Application Protection and Control			
15.1	Signature-based application control with patterns for thousands of applications	Comply		
15.2	Cloud Application Visibility and Control to discover Shadow IT	Comply		
15.3	App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added	Comply		
15.4	Micro app discovery and control	Comply		
15.5	Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level	Comply		
15.6	Per-user or network rule application control policy enforcement	Comply		
16	Web & App Traffic Shaping			
16.1	Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared	Comply		
17	Cloud Sandbox Protection			
17.1	Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)	Comply		
17.2	Aggressive behavioral, network, and memory analysis	Comply		
17.3	Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis	Comply		
17.4	Detects sandbox evasion behavior	Comply		
17.5	Machine Learning technology with scans all dropped executable files	Comply		

17.6	In-depth malicious file reports and dashboard file release capability	Comply		
17.7	Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis	Comply		
17.8	Supports one-time download links	Comply		
18	Email Protection and Control			
18.1	E-mail scanning with SMTP, POP3, and IMAP support	Comply		
18.2	Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology	Comply		
18.3	Block spam and malware during the SMTP transaction	Comply		
18.4	DKIM and BATV anti-spam protection	Comply		
18.5	Spam greylisting and Sender Policy Framework (SPF) protection	Comply		
18.6	Recipient verification for mistyped email addresses	Comply		
18.7	Second independent malware detection engine for dual-scanning	Comply		
18.8	Live Protection real-time in-the-cloud lookups for the latest threat intelligence	Comply		
18.9	Automatic signature and pattern updates	Comply		
18.10	Smart host support for outbound relays	Comply		
18.11	File-Type detection/blocking/scanning of attachments	Comply		
18.12	Accept, reject or drop over-sized messages	Comply		
18.13	Detects phishing URLs within e-mails	Comply		
18.14	Use pre-defined content scanning rules or create your own custom rules based on a variety of criteria with granular policy options and exceptions	Comply		
18.15	TLS Encryption support for SMTP, POP and IMAP	Comply		
18.16	Append signature automatically to all outbound messages	Comply		
18.17	Email archiver	Comply		

18.18	Individual user-based block and allow sender lists maintained through the user portal	Comply		
19	Email Quarantine Management			
19.1	Spam quarantine digest and notifications options	Comply		
19.2	Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages	Comply		
19.3	Self-serve user portal for viewing and releasing quarantined messages	Comply		
20	Email Encryption and DLP			
20.1	SPX encryption for one-way message encryption	Comply		
20.2	Recipient self-registration SPX password management	Comply		
20.3	Add attachments to SPX secure replies	Comply		
20.4	Completely transparent, no additional software or client required	Comply		
20.5	DLP engine with automatic scanning of emails and attachments for sensitive data	Comply		
20.6	Pre-packaged sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by	Comply		
21.	Web Application Firewall Protection			
21.1	Reverse proxy	Comply		
21.2	URL hardening engine with deep-linking and directory traversal prevention	Comply		
21.3	Form hardening engine	Comply		
21.4	SQL injection protection	Comply		
21.5	Cross-site scripting protection	Comply		
21.6	Dual-antivirus engines	Comply		
21.7	HTTPS (TLS/SSL) encryption offloading	Comply		

21.8	Cookie signing with digital signatures	Comply		
21.9	Path-based routing	Comply		
21.10	Outlook anywhere protocol support	Comply		
21.11	Reverse authentication (offloading) for form-based and basic authentication for server access	Comply		
21.12	Virtual server and physical server abstraction	Comply		
21.13	Integrated load balancer spreads visitors across multiple servers	Comply		
21.14	Skip individual checks in a granular fashion as required	Comply		
21.15	Match requests from source networks or specified target URLs	Comply		
21.16	Support for logical and/or operators	Comply		
21.17	Assists compatibility with various configurations and non-standard deployments	Comply		
21.18	Options to change Web Application Firewall performance parameters	Comply		
21.19	Scan size limit option	Comply		
21.20	Allow/Block IP ranges	Comply		
21.21	Wildcard support for server paths and domains	Comply		
21.22	Automatically append a prefix/suffix for authentication	Comply		
22	Firewall Reporting			
22.1	Pre-defined reports with flexible customization options	Comply		
22.2	Intuitive user interface provides graphical representation of data	Comply		
22.3	Report dashboard provides an at-a-glance view of events over the past 24 hours	Comply		
22.4	Easily identify network activities, trends, and potential attacks	Comply		
22.5	Easy backup of logs with quick retrieval for audit needs	Comply		
22.6	Simplified deployment without the need for technical expertise	Comply		

23	Warranty and Support - 36 Months			
23.1	Hardware warranty & RMA with Advanced Exchange	Comply		
23.2	24x7 Support via Telephone & Email	Comply		
23.3	FREE Security Updates & Patches	Comply		
23.4	FREE Software Features Updates & Upgrades	Comply		
24	Security Subscriptions - 36 Months			
24.1	Basic Firewall with VPN, Routing, WAN Link Load Balancing, Traffic Shaping & Quota, Wireless, Authentication, etc	Comply		
24.2	Intrusion Prevention, HTML5, Advanced Threat Protection, Anti-malware	Comply		
24.3	URL, AppCtrl, Web/App Traffic Shaping	Comply		
24.4	On-box antispam, Email Antivirus , Email Data loss prevention, Email Encryption	Comply		
24.5	Machine Learning and Sandboxing File Analysis, reporting	Comply		
24.6	Web Application Firewall for Web Server Protection	Comply		

.....
 Authorize Signature
 & Seal of the Firm