PART A

TENDER SUBMISSION

FORM A: TENDER
(SEE B7)

1. Project Title — SUPPLY AND INSTALLATION OF FIREWALL SYSTEM

2. Bidder

_____
Name of Bidder

_____
Street

_____
City Province Postal Code

(Mailing address if different)

_____
Street or P.O. Box

_____
City Province Postal Code

The Bidder is:

(Choose one)

☐ a sole proprietor

☐ a partnership

☐ a corporation

carrying on business under the above name.

3. Contact Person — The Bidder hereby authorizes the following contact person to represent the Bidder for purposes of the Bid.

_____
Contact Person Title

_____
Telephone Number Facsimile Number

4. Definitions — All capitalized terms used in the Contract shall have the meanings ascribed to them in the General Conditions and D3 unless the context otherwise requires.

5. Offer — The Bidder hereby offers to perform the Work in accordance with the Contract for the price(s), in Canadian funds, set out on Form B: Prices, appended hereto.

6. Subcontractors

The Bidder agrees that, if he subcontracts any portion of the Work, he shall employ only Subcontractors who have successfully carried out work similar in nature, scope and value to the portion of the Work proposed to be subcontracted to them, or who are fully capable of performing the Work required to be done in accordance with the terms of the Contract.

7. Contract

The Bidder agrees that the Tender Package in its entirety shall be deemed to be incorporated in and to form a part of this offer notwithstanding that not all parts thereof are necessarily attached to or accompany this Tender Submission.

8. Addenda

The Bidder certifies that the following addenda have been received and agrees that they shall be deemed to form a part of the Contract:

No. _____ Dated _____

_____ _____

_____ _____

9. Time

This offer shall be open for acceptance, binding and irrevocable for a period of thirty (30) Calendar Days following the Submission Deadline.

10. Signatures

In witness whereof the Bidder or the Bidder's authorized official or officials have signed this

_____ day of _____ , 20_____ .

Signed and sealed in the presence of:	Signature of Bidder or Bidder's Authorized Official or Officials
_____ (Witness)	_____
	_____ (Print here name and official capacity of individual whose signature appears above)
_____ (Witness)	_____
	_____ (Print here name and official capacity of individual whose signature appears above)

SEAL

FORM B: PRICES
(See B8)

SUPPLY AND INSTALLATION OF FIREWALL SYSTEM

UNIT PRICES

ITEM NO.	DESCRIPTION	SPEC. REF.	UNIT	APPROX. QUANTITY	UNIT PRICE	AMOUNT
1.	Hardware Appliance	E2	Each	2		
2.	Firewall Software	E3	Each	2		
3.	Vulnerability Testing	E4	Lot	1		
4.	Training	E5	Lot	1		
5.	Software Subscription	E6	Year	1		
6.	Hardware Support / Maintenance	E7	Year	1		

TOTAL BID PRICE (GST extra) (in figures) $ _____

(in words)_____

_____

_____
Name of Bidder

FORM N: COMPLIANCE CHECKLIST

	Description	Compliant Yes /No
	FIREWALL SPECIFICATIONS	
1	Must be EAL3+ approved appliance under the Common Criteria Evaluated Product List (products listed as undergoing evaluation for EAL3+ or higher may be considered as well)	
2	Must support a minimum of 6 10/100 Ethernet network connections. If additional interfaces are required for failover connections between the firewalls than those must be added as additional interfaces on top of the 6 required.	
3	Firewall throughput must be at least 500 Mbps (Megabits per second).	
4	Simultaneous connections must be at least 250,000 connections	
5	Firewall must have high availability option that will provide automatic failover in case of a hardware failure. This additional failover device must have identical specifications (numbers of ports and performance) as the main firewall.	
6	The failover procedure must be capable of synchronizing configuration changes between the two firewall devices automatically so that no manual intervention is required if one device fails over to the other.	
7	The firewall must be able to provide stateful failovers so that dropped connections are kept to an absolute minimum. The stateful failover mechanism must be real-time and report missing state updates for monitoring purposes.	
8	Firewall must support stateful packet inspection, NAT and port forwarding (port forwarding of UDP packets is a must)	
9	Firewall should support both 168-bit Triple DES (3DES) and 256-bit Advanced Encryption Standard (AES) encryption..	
10	Must have Unlimited User license	
11	Must have a security hardened operating system (non-MS Windows) and provide multi-level security	
12	Must have Time-based rules set management.	
13	Must have Integrated Application proxies such as HTTP, FTP, SMTP and others. The application proxies must allow fine control of the protocol (for example in the case of an FTP proxy the system should allow you do allow gets but deny puts).	
14	Must have HTTP proxy must be able to integrate with a URL and keyword Blocker and CVP content scanning gateway.	
15	Must have a user definable generic proxy.	
16	Must be able to secure DNS services through a split-DNS implementation with multiple zones and host entries or some other equivalent method.	
17	Must have Comprehensive Logging and audit capabilities.	
18	Must have Comprehensive On-line help via graphical user interface.	
19	Must be appliances (i.e.: security devices that bundle hardware and software with a secure embedded operating system).	
20	Must be compatible with third party web and email content scanning solutions.	
21	The firewall must be able to be expanded to allow the number of Ethernet ports required above plus any additional ports required for failover.	

22	The firewall must be able to be expanded to support gigabit ethernet ports (over fiber or copper cat5 cable) for future expandability.	
23	Must fit a standard 19" rack.	
24	Must be able to do static routing. The ease by which this is accomplished will be rated.	
25	Must be able to perform dynamic and static Network Address Translation. The size and capacity of the NAT table will be rated. NAT must also be able to be disabled or enabled on individual interfaces.	
26	Must provide secure remote administration of the firewall. (Describe what is required at the client workstation to accomplish this).	
27	Must have simple Administration interfaces.	
28	The proposed system(s) must have detailed logging (i.e.: Logging of all inbound connections whether they succeeded or failed. Logging of all outbound connections including all rejected connections. Logging of configuration changes. Logging of security controls changes).	
29	The proposed system(s) must have the ability to summarize data easily (type of traffic by day/week/month).	
30	The proposed system(s) must have auto alerts**.** Describe which methodologies are used to accomplish this (i.e.: Audio notification, Mail notification, Pager notification, SNMP notification)	
31	The proposed system(s) must have blocking of inbound and outbound traffic by IP Address.	
32	The proposed system(s) must have blocking of inbound and outbound traffic by Port number.	
33	The proposed system(s) must have blocking of inbound and outbound traffic by Protocol.	
34	Must describe any additional services or diagnostic tools available on the firewall (ie. traceroute, ping, etc.)	
35	Must provide telephone technical support 7 days per week, 24 hours per day, and 365 days per year.	
36	Must be proactive in the distribution of information to clients for security patches and maintenance upgrades. (Describe distribution methods)	
37	The proposed system(s) must integrate with third party anti-virus scanning products or appliance based AV solutions..	
38	Must provide Online Support (i.e.: FAQ, Knowledge Base, Discussion groups, Whitepapers)	
39	Must have Remote Browser based management via SSL	
40	Must have integrated remote management via SSH enabled client	
41	Must be able to forward firewall audit logs automatically to the following: SysLog server or FTP server	
42	Must be able to detect and log land attack (Denial of Service) and stop current sessions	
43	Must be able to detect and log Ping of death attacks and stop current sessions	
44	Must be able to detect and log TCP SYN flood attacks and stop current sessions	
45	Must have an integrated alerts management notification tools	
46	Must have an integrated alerts management notification tools	

47	Must have Alerts notification via Email or pager. Other optional notifications via SNMP or syslog servers may be considered as well.	
48	Must have an integrated log archiving tool	

_____
Name of Bidder