SURUHANJAYA PELABUHAN PULAU PINANG

KENYATAAN SEBUT HARGA

Tawaran adalah dipelawa daripada pembekal-pembekal tempatan yang berkelayakan dan berpengalaman serta berdaftar dengan Kementerian Kewangan dalam bidang berkaitan dan masih dibenarkan membuat tawaran bagi bekalan/perkhidmatan atau kerja seperti berikut.

NO. DAN TAJUK SEBUT HARGA	KOD BIDANG PENDAFTARAN	TARIKH/TEMPAT DIBEKALKAN DOKUMEN	TARIKH TUTUP
SEBUT HARGA BIL. 17/2018 PEMBEKALAN DAN PEMASANGAN FIREWALL DI PEJABAT SURUHANJAYA PELABUHAN PULAU PINANG	**210101/ 210102/ 210107**	25 Julai 2018 / Laman Web SPPP http://www.penangport.gov.my	8 Ogos 2018 Jam 12:00 tengahari

PERHATIAN

1. Sila lengkapkan borang tawaran (Borang A, Borang B dan Borang C). Borang-borang serta dokumen sokongan hendaklah dihantar ke pejabat Suruhanjaya Pelabuhan Pulau Pinang di alamat seperti berikut:-

   Pengurus Besar
   Suruhanjaya Pelabuhan Pulau Pinang
   Aras 2, Swettenham Pier Cruise Terminal
   No. 1A Pesara King Edward
   10300 George Town, Pulau Pinang

   (SILA MASUKKAN KE DALAM PETI SEBUT HARGA)

2. Sila rujuk kepada Senarai Semak sebelum menghantar semua dokumen sebut harga.

3. **Dokumen sebut harga hendaklah dimasukkan ke dalam satu sampul surat bertutup dan bertanda** SPESIFIKASI BAGI SEBUT HARGA BIL. 17/2018: PEMBEKALAN DAN PEMASANGAN FIREWALL DI PEJABAT SURUHANJAYA PELABUHAN PULAU PINANG.

4. Dokumen sebut harga hendaklah dimasukkan ke dalam Peti Sebut Harga di alamat seperti dinyatakan di atas sebelum atau pada 8 Ogos 2018, jam 12:00 tengah hari (TARIKH TUTUP SEBUT HARGA). Tawaran yang diterima selepas tarikh dan masa sebut harga ditutup akan ditolak.

5. Tempoh sahlaku sebut harga hendaklah 90 hari selepas tarikh tutup.

6. Pihak Suruhanjaya Pelabuhan Pulau Pinang tidak terikat untuk menerima mana-mana tawaran yang terendah.

Tarikh Iklan/Notis : 25 Julai 2018

Borang A

Bil.	Perihal barang-barang/perkhidmatan	Kuantiti	Harga Seunit (RM)	Harga (RM)
	SILA LIHAT DI LAMPIRAN A			

(Jika ruangan tidak mencukupi, sila kepilkan lampiran)

Ringgit Malaysia:

.....

i. *No. Pendaftaran dengan Kementerian Kewangan .....

ii. Harga yang ditawarkan adalah harga bersih; dan

iii. Tempoh membekalkan barang .....

Saya/Kami dengan ini menawarkan untuk membekalkan barang-barang/perkhidmatan seperti tersebut di atas dengan harga yang telah disertakan. Saya/kami akan mematuhi Syarat-syarat Am yang ditetapkan bagi pelawaan ini.

Tanda tangan penyebut harga .....

Tarikh :..... Nama : .....

Nombor Kad Pengenalan : .....

Alamat Syarikat :.....

.....

No. Tel. .....

Cop Syarikat :

*** No. Pendaftaran dengan Kementerian Kewangan perlu dinyatakan dengan mengikut Kod Bidang Pendaftaran yang telah dicatitkan di muka surat hadapan sebut harga ini. Sila sertakan sesalinan sijil pendaftaran dengan Kementerian Kewangan semasa penyerahan sebut harga tersebut.**

Mustahak - Lihat Syarat-syarat Am

SYARAT-SYARAT AM

Tertakluk kepada apa-apa syarat khas yang ditetapkan di tempat lain dalam pelawaan ini, syarat-syarat am yang berikut hendaklah dipakai, melainkan setakat mana syarat-syarat am itu ditolak atau diubah dengan khususnya oleh penyebut harga.

1. KEADAAN BARANG
   Semua barang hendaklah tulin, baru dan belum digunakan.

2. HARGA
   Harga yang ditawarkan hendaklah harga bersih termasuk semua diskaun dan kos tambahan yang berkaitan.

3. SEBUT HARGA SEBAHAGIAN
   Sebut harga boleh ditawarkan bagi semua bilangan item atau sebahagian bilangan item.

4. BARANG-BARANG SETARA
   Sebut harga boleh ditawarkan bagi barang-barang setara yang sesuai dengan syarat butir-butir penuh diberi.

5. PENYETUJUAN
   (i) SPPP tidak terikat untuk menyetujuterima sebut harga yang terendah atau mana-mana sebut harga.
   (ii) Tiap-tiap satu butiran akan ditimbangkan sebagai suatu sebut harga yang berasingan.

6. PEMERIKSAAN
   (i) SPPP adalah sentiasa berhak menghendaki barang-barang itu diperiksa atau diuji oleh seseorang pegawai yang dilantik olehnya dalam masa pembuatan atau pada bila-bila masa lain sebelum penyerahan.
   (ii) Penyebut harga hendaklah memberi kemudahan pemeriksaan atau pengujian apabila dikehendaki.

7. PERAKUAN MENYATAKAN PENENTUAN TELAH DIPATUHI
   Penyebut harga dikehendaki memperakui bahawa $\frac{\text{Barang-barang}}{\text{Perkhidmatan}}$ yang dibekalkan oleh mereka adalah mengikut penentuan atau piawai (jika ada) yang dinyatakan di dalam pelawaan ini.

8. PENOLAKAN
   (i) Barang-barang yang rendah mutunya atau yang berlainan daripada barang-barang yang telah dipersetujui sebut harganya boleh ditolak.
   (ii) Apabila diminta penyebut harga hendaklah menyebabkan barang-barang yang ditolak itu dipindahkan atas tanggungan dan perbelanjaannya sendiri, dan ia hendaklah membayar balik kepada Kerajaan segala perbelanjaan yang telah dilakukan mengenai barang-barang yang ditolak itu.
   (iii) Fasal-kecil (i) dan (ii) di atas ini tidaklah memudaratkan apa-apa hak SPPP untuk mendapatkan gantirugi kerana kemungkiran kontrak.

9. PENGIKLANAN
   Tiada apa-apa iklan mengenai persetujuan terhadap mana-mana sebutharga boleh disiarkan dalam mana-mana akhbar, majalah atau lain-lain saluran iklan tanpa kelulusan Suruhanjaya Pelabuhan Pulau Pinang terlebih dahulu.

10. TAFSIRAN

Sebut harga ini dan apa-apa kontrak yang timbul daripadanya hendaklah diertikan mengikut dan dikawal oleh undang-undang Malaysia, dan penyebutharga bersetuju tertakluk hanya kepada bidangkuasa Mahkamah Malaysia sahaja dalam apa-apa pertikaian atau perselisihan jua pun yang mungkin timbul mengenai sebutharga ini atau apa-apa kontrak yang timbul daripadanya.

11. INSURAN

Tiada apa-apa insuran atas barang-barang dalam perjalanan daripada negeri pembekal atau dalam Malaysia dikehendaki dimasukkan ke dalam sebutharga.

12. CUKAI

Harga yang ditawarkan adalah diertikan sebagai termasuk cukai jika berkenaan.

13. PEMBUNGKUSAN

(i) Harga yang ditawarkan adalah diertikan sebagai termasuk belanja bungkusan dan belanja pembungkusan.

(ii) Apa-apa kerugian atau kerosakan akibat bungkusan atau pembungkusan yang tidak mencukupi atau yang cacat, hendaklah diganti oleh penjual.

14. PENGENALAN

Nama pembuat, jenama, nombor perniagaan atau nombor katalog dan negeri tempat asal barang-barang itu, jika berkenaan, hendaklah ditunjukkan.

15. PENALTI LEWAT PENGHANTARAN

Penalti akan dikenakan terhadap pembekal sekiranya tidak dapat membuat penghantaran dalam tempoh masa yang ditetapkan.

Kadar penalti adalah seperti berikut:

$$\frac{18\%}{365} \text{ X jumlah nilai kontrak x bilangan hari yang lewat bekal}$$

BARANG-BARANG DIPESAN DARI LUAR MALAYSIA

16. CUKAI

Harga tawaran hendaklah diertikan sebagai termasuk semua cukai, unsur-unsur cukai adalah dikehendaki ditunjukkan berasingan.

17. MATAWANG

Sebut harga hendaklah dinyatakan dalam Ringgit Malaysia (RM).

18. PEMBUNGKUSAN

(i) Barang-barang hendaklah dibungkus dengan sesuai untuk dieksport ke Malaysia melainkan jika mengikut norma perdagangan barang-barang itu dieksport dengan tidak dibungkus.

(ii) Harga yang ditawarkan adalah diertikan sebagai termasuk belanja bungkusan dan belanja pembungkusan.

(iii) Apa-apa kerugian atau kerosakan akibat bungkusan atau pembungkusan yang tidak mencukupi atau cacat hendaklah diganti oleh penyebut harga.

Borang B
(SAP bertarikh 1 April 2010)

SURAT AKUAN PEMBIDA

Bagi

SEBUT HARGA BIL. 17/2018: PEMBEKALAN DAN PEMASANGAN FIREWALL DI PEJABAT SURUHANJAYA PELABUHAN PULAU PINANG

Saya, ...nombor kad pengenalan .....yang mewakili..... nombor Pendaftaran ..... dengan ini mengisytiharkan bahawa saya atau mana-mana individu yang mewakili syarikat ini tidak akan menawar atau memberi rasuah kepada mana-mana individu dalam Suruhanjaya Pelabuhan Pulau Pinang atau mana-mana individu lain, sebagai sogokan untuk dipilih dalam tender/sebut harga* seperti di atas. Bersama-sama ini dilampirkan Surat Perwakilan Kuasa bagi saya mewakili syarikat seperti tercatat di atas untuk membuat pengisytiharan ini.

2. Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati bersalah menawarkan atau memberi rasuah kepada mana-mana individu dalam Suruhanjaya Pelabuhan Pulau Pinang atau mana-mana individu lain sebagai sogokan untuk dipilih dalam tender/sebut harga* di atas, maka saya sebagai wakil syarikat bersetuju tindakan-tindakan berikut diambil:

2.1 penarikan balik tawaran kontrak bagi tender/sebut harga* di atas; atau

2.2 penamatan kontrak bagi tender/sebut harga* di atas; dan

2.3 lain-lain tindakan tatatertib mengikut peraturan perolehan Kerajaan.

3. Sekiranya terdapat mana-mana individu cuba meminta rasuah daripada saya atau mana-mana individu yang berkaitan dengan syarikat ini sebagai sogokan untuk dipilih dalam tender/sebut harga* seperti di atas, maka saya berjanji akan dengan segera melaporkan perbuatan tersebut kepada pejabat Suruhanjaya Pencegahan Rasuah Malaysia (SPRM) atau balai polis yang berhampiran.

Yang Benar,

Tanda tangan : .....

Nama : .....

No. Kad Pengenalan : .....

Cop Syarikat :

Catatan: * Potong mana yang tidak berkenaan.

Borang C

SENARAI SEMAK (BEKALAN/PERKHIDMATAN/KERJA)

Sila Tandakan [√] Bagi Dokumen-dokumen Yang Disertakan

Bil	Perkara/Dokumen	Untuk Ditanda Oleh Syarikat	Untuk Ditanda Oleh Jawatankuasa Pembuka Sebut Harga
1.	*Salinan Sijil Akuan Pendaftaran Dari Kementerian Kewangan (Bekalan/Perkhidmatan)	☐	☐
2.	Salinan Sijil Akuan Bumiputera Dari Kementerian Kewangan (Bekalan/Perkhidmatan)	☐	☐
3.	*Borang Sebut Harga Telah Diisi Dengan Lengkap (Termasuk nilai tawaran dan tempoh bekal) Dan Ditandatangani	☐	☐
4.	*Maklumat Penyebut Harga (Profil Syarikat)	☐	☐
5.	*Penyerahan Katalog	☐	☐
6.	*Salinan Penyata Bulanan Akaun Bank bagi Tiga (3) Bulan Terakhir (April, Mei & Jun 2018)	☐	☐
7.	*Surat Akuan Pembida (SPRM)	☐	☐

PENGESAHAN OLEH SYARIKAT

Dengan ini saya mengesahkan bahawa saya telah membaca dan memahami semua syarat-syarat dan terma yang dinyatakan di dalam dokumen sebut harga. Semua maklumat yang dikemukakan adalah benar.

Tanda tangan : .....

Nama : .....

Jawatan : .....

Tarikh : .....

UNTUK KEGUNAAN SURUHANJAYA PELABUHAN PULAU PINANG

Jawatankuasa Pembuka Sebut Harga mengesahkan penerimaan dokumen bertanda kecuali bagi perkara bil. .....(jika ada)

Tanda tangan:
Nama : .....
Tarikh : .....

Tanda tangan:
Nama : .....
Tarikh : .....

Tanda tangan:
Nama : .....
Tarikh : .....

Nota: Dokumen yang bertanda * adalah wajib disertakan dan dipatuhi semasa penghantaran dokumen sebut harga. Dokumen sebut harga yang tidak lengkap akan tidak dipertimbangkan.

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
A	**Next Generation Firewall**			
	Next Generation Firewall Quantity (2 Unit)	**M**		
1.0	**Product Details**			
1.1	Proposed next generation firewall brand	M		
1.2	Proposed next generation firewall model	M		
1.3	Location of proposed firewall: 1. **Ibu Pejabat SPPP:** **Aras 2, Swetthenham Pier Cruise Terminal,** **No. 1A, Pesara King Edward, 10300** **Pulau Pinang** 2. **Pejabat SPPP Butterworth:** **Free Commercial Zone Unit** **Suite 1, Level 2, NB Tower,** **5050 Jalan Bagan Luar,** **12000 Butterworth, Penang.**	M		
2.0	**Platform & Performance Capabilities**			
2.1	The proposed firewall shall be an appliance-based next generation firewall with built-in SSD drive capable of supporting at least 240GB storage space	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
2.2	The vendor shall propose the solution with the capability to support **at least 940 Mbps** of application firewall throughput.	M		
2.3	The proposed hardware appliance shall support at least **610 Mbps** of threat prevention throughout with IPS, Antivirus, Antispyware, URL filtering, File Blocking, Advance Persistence Threat (APT) protection and application awareness enabled concurrently. Such performance should not further decrease due to enablement of any function mentioned above. ie: Enabling Antivirus scanning will not decrease the hardware performance as compared to enabling IPS. The proposed hardware should not have limitations of operating under specific mode or security signatures to preserve the performance or enabling certain functionality	M		
2.4	The proposed solution shall support at least **128,000** concurrent sessions	M		
2.5	The proposed solution shall support at least **8,300** new sessions per second	M		
2.6	The proposed solution shall support at least **400 Mbps** of **IPSEC VPN** throughput	M		
2.7	The proposed hardware shall come with at least **4 x 10/100/1000 RJ45** network ports.	M		
2.8	The proposed hardware shall support at least **8 x 1GE SFP ports**	M		
2.9	The proposed solution shall support at least **30 security zones**	M		
3.0	**Technology Architecture**			
3.1	The solution hardware architecture must be optimized for layer 7 application content processing and have special ASICS to handle signature matching and processing in parallel fashion.	M		
3.2	The hardware architecture shall have control and data plane at the hardware / software level. Bidders are required to provide detail clarification how a packet would be treated when it is subjected to content inspection	M		
4.0	**Networking**			

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
4.1	The solution must be able to support policy-based Network Address Translation (NAT) capabilities: • Port Address Transation • Dynamic IP/Port NAT • Static IP NAT	M		
4.2	The solution must be able to provides NAT traversal capabilities, supporting VOIP application and services.	M		
4.3	The solution must be able to support policy-based Traffic Management QoS based on applications. Note: Application must not be interpreted as port service	M		
4.4	The solution must be able support the following routing protocols: • Static • RIP • OSPF • BGP	M		
4.5	The solution shall support the following deployment mode: • Tap mode (via mirrored or SPAN port) • Layer 2 mode • Layer 3 mode • Transparent mode (layer 1 or bump on the wire)	M		
4.6	The solution shall support concurrent use of vwire, tap mode, L2 and L3 within the same device.	M		
4.7	The solution shall support 802.1Q VLAN tagging (in tap, transparent, layer 2 and layer 3)	M		
4.8	The solution shall support standard based IEEE 802.3ad link aggregation	M		
4.9	The solution shall support 8 links per LACP group	M		
4.10	The solution shall support up to 4 ECMP links	M		
4.11	The solution shall support Dual Stack IPv4 / IPv6 application control and threat inspection in any of the deployment mode: Tap Mode, VWire mode, Layer2 mode, Layer 3 mode.	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
4.12	The solution shall support Policy Based forwarding based on the following: - Zone - Source or Destination Address - Source or destination port - Applications (not port-based) - AD/LDAP user or User Group	M		
4.13	The solution shall support Failure detection with BFD	M		
4.14	The solution shall support Per VLAN Spanning Tree (PVST+) BPDU rewrite	M		
5.0	**DOS Protection**			
5.1	The proposed next generation firewall must be able to support TCP reassembly for fragmented packet protection	M		
5.2	The proposed next generation firewall must be able to support Brute force attack mitigation	M		
5.3	The proposed next generation firewall must be able to support SYN cookie protection	M		
5.4	The proposed next generation firewall must be able to support IP spoofing	M		
5.5	The proposed next generation firewall must be able to support Malformed packet protection	M		
6.0	**High Availability**			
6.1	The proposed next generation firewall overall solution should support High Availability.	M		
6.2	The proposed next generation firewall shall come with dedicated HA ports that are not included in the number of interfaces mentioned in the earlier section.	M		
6.3	The proposed next generation firewall shall support both active/active and active/passive HA configuration	M		
6.4	The proposed next generation firewall shall capable of detecting link and path failure in addition to device failure	M		
6.5	The propose next generation firewall shall be capable of supporting encryption of HA heartbeat and control traffic	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
6.6	The proposed next generation firewall shall synchronize all sessions, decryption certificates, all VPN security associations, all threat and application signatures, all configuration changes and Forwarding Information Base (FIB) tables for HA	M		
6.7	The proposed next generation firewall in HA Active/Active setup shall be able to sychronize applications session even in asynchronous gateway environment.	M		
7.0	**Device Management**			
7.1	The proposed next generation firewall shall provide management interfaces as a single view to manage security policies, network configurations (Eg routing table, interface setup) not limited to: • Web-based Graphical User Interface (GUI) • Command-Line Interface (CLI)	M		
7.2	The proposed next generation firewall shall come with dedicated Out-Of-Band Management Port	M		
7.3	The proposed next generation firewall shall support role-based adminitrative access to allow delegates specific tasks or permissions to certain administrators	M		
7.4	The proposed next generation firewall shall support schedule log exports using SCP or FTP protocol.	M		
7.5	The proposed next generation firewall shall be administered locally on the appliance without additional management or logging software.	M		
8.0	**Policy Based Control**			
8.1	The proposed next generation firewall shall support all the following in a single policy: • policy control by port and/or protocol; • policy control by source/destination zone; • policy control based on application or application category; • policy control by URL category; • policy control based on user or user group;	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
	• policy control based on IP address; • policy control by country code; • policy control by machine state;			
8.2	The proposed next generation firewall security policy shall support IPv4 and IPv6 objects (concurrently on a single rule);	M		
8.3	The proposed next generation firewall security policy shall support multicast rules/objects	M		
8.4	The proposed next generation firewall security policy shall scheduled time of day enablement based on criteria below: • Daily recurrence • Weekly recurrence • Specific date and time	M		
8.5	The proposed next generation firewall shall support external dynamic block list for a text file that contains a list of IP addresses, IP ranges, or IP subnets, and is hosted in a form of web server. The dynamic block list can be used to deny or allow access from the next generation firewall if the users/hosts traffic hits the security policy.	M		
9.0	**Application Security Policy**			
9.1	The proposed next generation firewall shall support network traffic classification, which identifies applications across all ports irrespective of port/protocol/evasive tactics.	M		
9.2	The proposed next generation firewall shall have multiple mechanisms for classifying applications and application identification technology	M		
9.3	The proposed next generation firewall shall have application identification technology based upon IPS or deep packet inspection	M		
9.4	The proposed next generation firewall shall support custom application signatures. It shall support multiple parameters and NOT limited to URL only.	M		
9.5	The proposed next generation firewall shall be able to automatically include all the default ports required by the application. No other ports shall be open unless explicitly	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
	configured.			
9.6	The proposed next generation firewall shall have the option to auto generate packet capture for all unknown applications to facilitate custom application signature creation.	M		
9.7	The proposed next generation firewall shall be able to define the regions and countries in the security policies.	M		
9.8	The proposed next generation firewall shall include a searchable list of currently identified applications with explanation and links to external sites for further clarification.	M		
9.9	The proposed next generation firewall shall allow dynamic updates of the application database (DB) and not require a service restart or reboot.	M		
9.10	The proposed next generation firewall shall warn the end-user with a customizable page when the application is blocked.	M		
9.11	The proposed next generation firewall shall delineate specific instances of peer2peer traffic (Bittorrent, emule, neonet, etc.)	M		
9.12	The proposed next generation firewall shall delineate specific instances of instant messaging (AIM, YIM, Facebook Chat, etc.)	M		
9.13	The proposed next generation firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability	M		
9.14	The proposed next generation firewall shall delineate specific instances of Proxies (ultrasurf, ghostsurf, freegate, etc.)	M		
9.15	The proposed next generation firewall shall be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.	M		
9.16	The proposed next generation firewall shall support user-identification allowing Active Directory, LDAP, RADIUS groups, or users to access a particular application, while denying others	M		
10.0	**Integrated Intrusion Prevention System**			
10.1	The proposed next generation firewall shall support IPS security function, antivirus and anti-spyware.	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
10.2	The proposed next generation firewall shall use stream based antivirus and anti-spyware and not store-and-forward traffic inspection.	M		
10.3	The proposed next generation firewall shall support built-in packet capturing of specific threats for forensic evidence or investigation.	M		
10.4	The proposed next generation firewall shall block known network and application-layer vulnerability exploits.	M		
10.5	The proposed next generation firewall shall provide the ability to allow the organization to write its own customized threat signatures for new or targeted threats that may not be found in other environments.	M		
10.6	The proposed next generation firewall shall able to analyse all DNS queries and request. It shall block any DNS request or query to blacklisted or malicious domains.	M		
10.7	The proposed next generation firewall shall have the capability to sinkhole DNS request for blacklisted or malicious Domains to a configured destination IP address.	M		
10.8	The proposed next generation firewall shall have the capability to define different antivirus / vulnerability protection / antispyware action templates for each security policies defined.	M		
10.9	The proposed next generation firewall shall be able to perform Anti-virus scans for SMB traffic	M		
10.10	The proposed next generation firewall support attack recognition for IPv6 traffic the same way it does for IPv4	M		
10.11	The proposed next generation firewall shall support be able to exclude certain hosts from scanning of particular signatures	M		
10.12	The proposed next generation firewall shall support granular tuning with option to configure overrides for individual signatures	M		
10.13	The proposed next generation firewall shall support several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
10.14	The proposed next generation firewall shall support response adjustment on a per signature basis.	M		
10.15	The proposed next generation firewall shall support the prevention of credential theft without solely using Phishing category websites prevention only. If the answer is “C” , please elaborate how the proposed platform prevent credential theft.	M		
11.0	**Modern Malware Protection**			
11.1	The proposed next generation firewall shall support sandbox-based protection of unknown viruses	M		
11.2	The proposed next generation firewall shall not further degrade threat prevention (IPS, Antivirus, & Antispyware, URL) throughput when the modern malware protection feature is turn on at the same time.	M		
11.3	The proposed next generation firewall shall support automated signature generation for discovered zero-day/advance malware for not more than 5 minutes	M		
11.4	The proposed next generation firewall shall support the protection against modern malware via behavioral analysis regardless of ports or encryption, with full visibility into all application, including web traffic (HTTP and SSL), email protocols (SMTP, IMAP, POP), FTP and SMB.	M		
11.5	The modern malware protection shall able to analyze the following file types: - • HTTP/HTTPS email links contained in SMTP and POP3 email messages) • Adobe Flash applets and Flash content embedded in web pages • Android Application Packages (.APK) • Portable Document Format • Java Applet (JAR/Class file types) • Portable Executables, which includes executable files, object code, DLLs, FON (fonts) • Microsoft Office files including documents (doc, docx, rtf), workbooks (xls, xlsx), PowerPoint (ppt, pptx) and Office Open XML (OOXML) 2007+ documents	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
11.6	The modern malware protection shall have Anti VM aware malware analysis environment to minimize the chance of sandbox bypass.	M		
11.7	The proposed next generation firewall shall support inline control (block/drop) of malware infection, botnet, command/control traffic	M		
11.8	The proposed next generation firewall shall have the ability to provide a comprehensive analysis report that includes the following:	M		
11.8.1	The detailed behavior exhibited by the unknown malware in the simulated environment, and the corresponding severity level of each of these behavior patterns	M		
11.8.2	Network activities conducted by the unknown malware in the simulated environment, including accessing other hosts on the network, DNS queries, and phone-home activity.	M		
11.8.3	Host activities performed by the unknown malware in the simulated environment, including process/file/registry-related activities as well as mutex creations	M		
11.8.4	Play-by-play list of the sequence of events that occurred during the unknown malware analysis.	M		
12.0	**URL Filtering**			
12.1	The proposed next generation firewall shall support integrated URL filtering/categorization	M		
12.2	The proposed next generation firewall shall support custom URL-categorization	M		
12.3	The proposed next generation firewall shall support block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time)	M		
12.4	The proposed next generation firewall shall enforce Safe Search to prevent inappropriate content from appearing in users' search results. The supported safe search engine shall not limited to Google, Yahoo or Bing.	M		
12.5	The proposed next generation firewall shall support Drive-by-	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
	download control to prevent download/upload of executable files from malicous web sites.			
12.6	The proposed next generation firewall shall support bandwidth control for designated categories by creating QoS policies for specified URL categories to control bandwidth consumption.	M		
12.7	The proposed next generation firewall shall support deployment flexibility to provide unlimited user license behind each URL filtering subscription without worrying about cost variations associated with user-based licensing.	M		
12.9	The proposed next generation firewall shall support logging of HTTP fields such as User-Agent, Referrer and X-Forwarder-For (XFF).	M		
12.10	The proposed next generation firewall shall support the ability to provide full-path categorization of the URLs and categorize content down to the page level instead of just at the directory level.	M		
13.0	**Data Filtering**			
13.1	The proposed next generation firewall shall support identification and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)	M		
13.2	The proposed next generation firewall shall support compressed information stored in zipped format and be able to unpack and filter per policy	M		
13.3	The proposed next generation firewall shall be capable of identifying and optionally preventing the transfer of files containing sensitive information (i.e. credit card numbers) via regular expression	M		
14.0	**User Identification Control**			
14.1	The proposed next generation firewall shall support authentication services for user-identification:	M		
14.1.1	Active Directory / LDAP	M		
14.1.2	Novell eDirectory	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
14.1.3	RADIUS	M		
14.1.4	Kerberos	M		
14.1.5	Client Certificates	M		
14.2	The proposed next generation firewall should support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP	M		
14.3	The proposed next generation firewall shall support user-identification without installing an agent on individual endpoints	M		
14.4	The proposed next generation firewall shall support user-identification from Citrix and terminal services environments in policy and logs	M		
14.5	The proposed next generation firewall shall populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time	M		
14.6	The proposed next generation firewall shall support terminal services such Citrix XenAPP or Microsoft Terminal Services for user identifications mapping.	M		
14.7	The proposed next generation firewall shall support Syslog Listener to natively harvest user information from 3rd Party Vendors.	M		
14.8	The proposed next generation firewall shall offer XML API to integrate user information into the security policies from other user directories, and authentication mechanisms.	M		
15.0	**Virtual Private Networking (VPN)**			
15.1	The proposed next generation firewall shall support standard-based IPSEC VPN connectivity for Site-to-SiteM VPN tunnel.	M		
15.2	The proposed next generation firewall shall support secure tunnel for remote users via SSL- or IPSEC-based VPN connection.	M		
15.3	The authentication mechanisms for secure remote users VPN connection shall support local DB, RADIUS, LDAP, Active Directory, Kerberos or smart cards	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
15.4	The SSL VPN client software must at least to support the following OS platform: • Apple Mac OS 10.6 or above • Apple IOS 6.0 or above • Windows XP, Vista, 7, 8 and 10 • Windows Surface Pro • Google Android 4.0.3 or above	M		
15.5	The SSL VPN remote agent must be able to provide host-based access control such as collect information about the security status of the end hosts - whether it has the latest security patches and antivirus definitions installed, have disk encryption enabled, the device is jailbroken or rooted (mobile devices only), or whether it is running specific software require within the organization, including custom applications—and base on the decision as to whether to allow or deny access to a specific host based on adherence to the host policies has been defined.	M		
15.6	The proposed next generation firewall shall support at least 1,000 Client based VPN users concurrently	M		
15.7	The proposed next-generation firewall shall support 2 factor authentication for SSL VPN connection	M		
15.8	The proposed next-generation firewall shall automate the creation of client certificate using Simple Certificate Enrollment Protocol (SCEP)	M		
16.0	**SSL/SSH Decryption**			
16.1	The proposed next generation firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	M		
16.2	The proposed next generation firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection	M		
16.3	The proposed next generation firewall shall be able to identify, decrypt and evaluate SSH / SSH Tunnel traffic in an outbound connection	M		
16.4	The proposed next generation firewall shall be able to identify, decrypt and evaluate SSH / SSH Tunnel traffic in an	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
	inbound connection			
16.5	The proposed next generation firewall shall be able to decrypt in tap, transparent, layer 2 and layer 3 deployment mode.	M		
16.6	The proposed next generation firewall shall support SSL decryption policies by allowing encrypted access to specific web sites about topics your employees enjoy – like health, finance, and shopping – while decrypting traffic to all other sites such as malware, forums, and entertainment sites.	M		
17.0	**Quality of Service (QoS)**			
17.1	The proposed next generation firewall shall support QoS tagging creation or edit on each individual security policy.	M		
17.2	The proposed next generation firewall should support the ability to create QoS policy on a per rule basis: • by source address • by destination address • by user/user group as defined by AD • by application (such as Skype, Bittorrent, YouTube, azureus) • by static or dynamic application groups (such as Instant Messaging or P2P groups) • by port	M		
17.3	The proposed next generation firewall shall define QoS traffic classes with: • guaranteed bandwidth • maximum bandwidth • priority queuing	M		
18.0	**Real-Time Security Dashboards, Logging & Reporting**			
18.1	The proposed next generation firewall shall provide graphical summary of the applications, users, URLs, threats and content traversing the networks.	M		
18.2	The next generation firewall allow administrator to drill down into applications detected and provide further information such as a description of the application or threat, an	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
	application behavioral charateristics, details on users using an application, details on those affected by threats.			
18.3	The proposed next generation firewall shall be able to present in a comparative statistics view based upon time frames, applications, application categories, threats profiles and threats attacker/victims based on geographical maps.	M		
18.4	The proposed next generation firewall shall offer log viewer that support context and expression-based filtering	M		
18.5	The proposed next generation firewall logs shall be exportable to a CSV file for further analysis	M		
18.6	The proposed next generation firewall shall contain User and Application information pertaining to the corresponding events across all types of logs (eg. traffic, security, url).	M		
18.7	The proposed next generation firewall shall be able to produce the following reports (without the need for additional software/hardware):	M		
18.7.1	Application Usage – Bytes and Sessions	M		
18.7.2	Threat Trends	M		
18.7.3	Correlated Reports – Application/Threats/URL	M		
18.7.4	Individual User ID or User Group usage report - Application/Session/Time/URL	M		
18.7.5	Botnet Report	M		
18.7.6	Built-in analytic tool uses logs in the next generation firewall that able to pinpoints areas of risks such as compromised hosts on the network in an automated way.	M		
18.7.7	The proposed next generation firewall shall be able to send out all the reports above in a scheduled manner to designated email addresses (without the need for additional software subscription/licenses or hardware components).	M		
18.7.8	The proposed next generation firewall shall have a capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) basis without the need of any additional software subscription/licenses or hardware components.	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
19.0	**Product Certification & Recognition**			
19.1	The proposed next generation firewall must be in the "**Leaders**" Quadrant in **Gartner's Magic Quadrant Enterprise Network Firewall** category for consecutive **5** years.	M		
B.	**Network Switch**			
	Network Switch Quantity (1 Unit)	M		
1.0	**Layer 2 manageable switches**			
	Product details			
1.1	Proposed switch brand	M		
1.2	Proposed switch model	M		
2.0	**Platform & Performance Capabilities**			
2.1	Proposed switch must come with at least48 x 10/100/1000Mbps ,4 SFP uplink interfaces.	O		
2.2	Proposed switch must supporting at least 128MB Flash memory	O		
2.3	Propose switch must supporting at least 512 DRAM	O		
2.4	Propose switch must supporting at least APM86392 600 MHz dual core	O		
2.5	Propose switch must supporting USB (Type B), Ethernet (RJ-45)	O		
2.6	Propose switch must supporting at least 108Gbps forwarding bandwidth	O		
2.7	Propose switch must supporting at least 216Gbps switching bandwidth	O		
2.8	Propose switch must supporting at least 1023 active VLANs	O		
2.9	Propose switch must supporting at least 4096 VLAN IDs	O		
2.10	Propose switch must supporting at least 16,000 unicast MAC addresses	O		
2.11	Propose switch must supporting at least 1000 IPv4 multicst routes and IGMP groups	O		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
2.12	Propose switch must supporting at least 500 IPv4 & IPv6 QoS ACEs	O		
2.13	Propose switch must supporting eight egress queues per port for QoS	O		
2.14	IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) provide rapid spanning-tree convergence independent of spanning-tree timers and also offer the benefit of Layer 2 load balancing and distributed processing	O		
2.15	Per-VLAN **Rapid** Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances.	O		
2.16	Dynamic Trunking Protocol (DTP) facilitates dynamic trunk configuration across all switch ports.	O		
C	**PDU**			
1.0	Install, Supply, testing Rack PDU, Basic, Zerou, 16A,230V,(20) C13 and (4) (C19) 1EC C20 **Quantity = 1 Unit**	M		
2.0	Custom Made 10 gang B5,363 13A Power Strip PDU with 16Amp DP MCB : Input IEC320 C13 plug with 2 meter cable **Quantity = 1 Unit**	M		
D	**Professional Services**			
1.0	**Scope of Work**			
	Tenderer shall propose suitable deployment method to PPC.			
1.1	Tenderer shall deploy NGFW firewall at SPPP HQ & SPPP NB Tower.	O		
1.2	**Deployment:-** • Configuration and implementation of NGFW • Process includes licensing, dynamic updates, and	O		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
	product registration • Create security rules and up to fifteen NAT rules • App-ID migration of commonly used ports (includes initial review of high-volume/multi-usage ports 80 & 443) • Enable threat protection content with up to one each of anti-virus, anti-spyware, vulnerability • Enable Wildfire security profile, note Wildfire license required • User-ID configuration with Active Directory • Setup Best Practice URL Security Policies			
2.0	**Warranty and Support**			
2.1	To provide 1 year of hardware warranty / maintenance services with 24 x 7 and 4 hours on-site response. All maintenance costs such as labor and parts are included / covered.	M		
2.2	Technical Support (Unlimited number of Email & Phone Support - may place calls 7 days per week, 24 hours per day, 365 days per year)	M		
2.3	Tendere shall proactively provide notifications of patches, bugs or firmware release to IT Operation team of PPC.	M		
2.4	Tender shall provides Onsite Incident support (Please provide plan and SLA)	M		
2.5	Tendere shall provide Advanced Hardware Replacement Program for 1 year (Please provide plan and SLA)	M		
2.6	Tenderer shall to carry out preventive maintenance at least twice per year over the 1 year period which includes Software/Firmware Upgrade for all hardware provided in this tender (Please provide Preventive Maintenance plan)	M		
2.7	Please specify and provide the after sales service plan for support and maintenance. (eg. Support flow chart)	M		
E	**Product Certified Training**			
1.0	The certified training programme must be conducted by the certified trainer from the manufacturer or appointed authorized training partner.	M		

	Specification	Mandatory (M) / Optional (O)	Yes/No	Tenderers Response
2.0	The certified training programme shall covers the scope on next generation firewall and centralized management systems.	M		
3.0	The certified training programme shall be included for 2 pax in any authorized training center for minimum 3 full days.	M		

LAMPIRAN B

KLAUSA PENCEGAHAN RASUAH DALAM DOKUMEN PEROLEHAN KERAJAAN

“Termination on Corruption, Unlawful or Illegal Activities

(a) Without prejudice to any other rights of the Government, if the [Company/Firm], its personnel, servants or employees is convicted by a court of law for corruption or unlawful or illegal activities in relation to this [Agreement/Contract] or any other agreement that the [Company/Firm] may have with the Government, the Government shall be entitled to terminate this [Agreement/Contract] at any time, by giving immediate written notice to that effect to the [Company/Firm].

(b) Upon such termination, the Government shall be entitled to all losses, costs, damages and expenses (including any incidental costs and expenses) incurred by the Government arising from such termination.

(c) For the avoidance of doubt, the Parties hereby agree that the [Company/Firm] shall not be entitled to any form of losses including loss of profit, damages, claims or whatsoever upon termination of this [Agreement/Contract].”