भारतीय प्रौद्योगिकी संस्थान गाँधीनगर
विश्वकर्मा शासकीय अभियांत्रिकी महाविद्यालय परिसर,
चाँदखेडा, अहमदाबाद, गुजरात - 382 424
INDIAN INSTITUTE OF TECHNOLOGY GANDHINAGAR
Vishwakarma Government Engineering College Campus,
Chandkheda, Ahmedabad, Gujarat - 382 424

Office : +91 93 2847 4216
Fax : +91 79 2397 2583
E-mail : office@iitgn.ac.in
website : http://www.iitgn.ac.in

IIT GN

Date – 26th February, 2016

CORRIGENDUM-I

Tender No. IITGN/ADVT/COMP/LTA/2015-16/0440 Dated 12th February, 2016

A) Under the Architecture Section clause no. 1.8, the points should be read as

Proposed appliance should contain

- 4 or more ports enabled of 1G Copper
- 4 or more ports enabled of 1G Fibre
- 4 or more ports enabled of 10G Fibre

Provide 4 nos of 10G and 4 nos of 1G SFP+ Fibre pluggable modules additionally.
Applicance must be ready or support with 4 nos of 40G QSFP ports from Day-1.

B) 4 Gbps or above Fully Protected throughput i.e. with IPS, Firewall, VPN, Web Intelligence services enabled and NGTP throughput 2 Gbps or above is required from Day-1

C) The proposed solution must work as an integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS and Web Application Firewall. Option to enable / disable any service.

D) The proposed solution must support Single Sign On for user authentication. SSO must be proxy independent.

E) The proposed solution should be able to force-logout users upon session time-out, web-based category and idle time-out.

F) The solution should be able to address all aspects of the Advanced Persistent Threat (APT) lifecycle, including: Blocking known malware sources, blocking known malware, identifying and blocking unknown or zero-day malware within an hour, protecting against client-side vulnerabilities, blocking command and control back-door traffic, blocking server-side vulnerabilities, and advanced application and user control within appliance or in Cloud

G) The proposed solution must support sandbox behaviour based inspection and protection of unknown viruses and malware within appliance or in Cloud

H) The proposed solution should support scanning for SMTP, POP3, FTP, HTTP, HTTPS, FTP over HTTP protocols.

I) The proposed solution must support on-appliance quarantine or remove facility/ dedicated quarantine or remove facility.

J) The proposed solution should be ICSA certified

K) The proposed solution must support authentication to comply with Internet Privacy laws, under Goverment of India Cyber Laws

L) The proposed solution should support Syslog, SNMP or must have integrated granular reporting solution.

M) The proposed solution should allow exporting of reports in PDF, Excel(optional)(preferred) and CSV format(preferred) and HTML.

N) Below points are also included under Application Control Section.

- Solution should support Application Control and URL filtering.
- Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc.
- Should support User and Group based policies

भारतीय प्रौद्योगिकी संस्थान गाँधीनगर
विश्वकर्मा शासकीय अभियांत्रिकी महाविद्यालय परिसर,
चाँदखेडा, अहमदाबाद, गुजरात - 382 424
INDIAN INSTITUTE OF TECHNOLOGY GANDHINAGAR
Vishwakarma Government Engineering College Campus,
Chandkheda, Ahmedabad, Gujarat - 382 424

Office : +91 93 2847 4216
Fax : +91 79 2397 2583
E-mail : office@iitgn.ac.in
website : http://www.iitgn.ac.in

IIT GN

Clarification(s) counter to queries from various vendors for the supply of "Firewall Device with Warranty"

Q1: Under the Architecture Section clause no. 1.9, you have asked for "4 Gbps or above Fully Protected throughput i.e., with Antivirus, IPS, Firewall, VPN, Web application firewall services enabled" - Request you to change the throughput value to be changed to 2 to 2.2 Gbps enabling NGTP features or to mention 4 Gbps with FW,VPN,IPS with Web Intelligence services enabled.

- Please refer point – B in above Corrigendum. Other points remain unaltered.

Q2: Under the Architecture Section clause no. 1.11, you have asked for "The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS and Web Application Firewall. Option to enable / disable any service." - Request for clarification on usage of Applications as Proxy Server.

- Please refer point – C in above Corrigendum. As of now we are not looking for HTTP proxy server but in the future we may explore.

Q3: Under the Admin/Auth Section clause no. 2.5, you have asked for "The proposed solution must support Single Sign On for user authentication. SSO must be proxy independent and should support all applications for authentication" - Request you to ammend as "The proposed solution must support Single Sign On for user authentication. SSO must be proxy independent. Also need clarity on list of applications"

- Please refer point – D in above Corrigendum. List of applications are all engineering, science, accounts software installed within the network.

Q4: Under Admin/Auth Section clause no. 2.9, you have asked for "The proposed solution should be able to force-logout users upon session time-out, quota exceeded (over download) and idle time-out." - In the available solution, Download by MB per user quota is not supported. Request you to ammend as Time-based and Web category based quota.

- Please refer point – E in above Corrigendum.

Q5: Under the Admin/Auth Section clause no. 2.13, you have asked for "The proposed solution must support MAC based user authentication" - Request you to omit this point.

- This point is omitted.

Q6: Under the Firewall Section clause no. 4.12, you have asked for "The solution should be able to address all aspects of the Advanced Persistent Threat (APT) lifecycle, including: Blocking known malware sources, blocking known malware, identifying and blocking unknown or zero-day malware within an hour, protecting against client-side vulnerabilities, blocking command and control back-door traffic, blocking server-side vulnerabilities, and advanced application and user control" - It is advised that the proposed feature should be cloud based.

- Please refer point – F in above Corrigendum.

Q7: Under the Firewall Section clause no. 4.13, you have asked for "The proposed solution must support sandbox behaviour based inspection and protection of unknown viruses and malware" - Would appreciate of the proposed solution must support sandbox behaviour based inspection and protection of unknown viruses and malware within appliance or in Cloud

- Please refer point – G in above Corrigendum.

भारतीय प्रौद्योगिकी संस्थान गाँधीनगर
विश्वकर्मा शासकीय अभियांत्रिकी महाविद्यालय परिसर,
चाँदखेडा, अहमदाबाद, गुजरात - 382 424
INDIAN INSTITUTE OF TECHNOLOGY GANDHINAGAR
Vishwakarma Government Engineering College Campus,
Chandkheda, Ahmedabad, Gujarat - 382 424

Office : +91 93 2847 4216
Fax : +91 79 2397 2583
E-mail : office@iitgn.ac.in
website : http://www.iitgn.ac.in

IIT GN

Q8: Under the Antivirus Section clause no. 6.1, you have asked for "The proposed solution should have an ICSA / West Coast Labs Checkmark certified" - Request you to omit this point from AV perspective.

- This point is omitted only from Antivirus perspective.

Q9: Under the Antivirus Section clause no. 6.2, you have asked for "The proposed solution should support scanning for SMTP, SMTPS, POP3, IMAP, FTP, HTTP, HTTPS, FTP over HTTP protocols." - Request you to rephrase the statement as "The proposed solution should support scanning for SMTP, POP3, FTP, HTTP, HTTPS, FTP over HTTP protocols."

- Please refer point – H in above Corrigendum.

Q10: Under the Antivirus Section clause no. 6.4, you have asked for, "The proposed solution must support on-appliance quarantine facility / dedicated quarantine facility and also a personalized user-based quarantine area" - Request you to rephrase the statement as "The proposed solution must support on-appliance quarantine or remove facility/ dedicated quarantine or remove facility."

- Please refer point – I in above Corrigendum.

Q11: Under the VPN Section, you have asked for "The proposed solution should be VPNC Basic interop and AES certified also should have an ICSA." - In our appliance can form tunnel with different brands & even can share documents for well-known brands but it is not VPNC certified. Our solution is VPN & ICSA certified.

- Please refer point – J in above Corrigendum.

Q12: Under the VPN Section clause no. 8.11, you have asked for "The proposed solution must provide on-appliance SSL VPN solution with Web Access (Clientless), Web Application Access (Most common used protocols), Full Tunnel and Split Tunnel control. Solution should provide per user / group SSL VPN access (Which involves free license for unlimited users)" - Request you to ammend the same as "The proposed solution must provide on-appliance SSL VPN solution with Web Access (Clientless), Web Application Access (Most common used protocols), Full Tunnel and Split Tunnel control. Solution should provide per user / group SSL VPN access (Which involves free license for the users). Please mention concurrent number of users as SSL works on concurrency and applicance has to be sized for the same."

- Please refer clause 1.9 under Section Architecture of Annexure-1.

Q13: Under Log/reporting Section clause no. 9.1, you have asked for "The proposed solution must support authentication to comply with Internet Privacy laws" - Please mention the laws.

- Please refer point – K in above Corrigendum.

Q14: Under the Log/reporting Section clause no. 9.3, you have asked for "The proposed solution should be able to be integrated with any reporting solution." - Request you to ammend as "The proposed solution should support Syslog, SNMP or must have integrated granular reporting solution"

- Please refer point – L in above Corrigendum.

Q15: Under Logging and reporting section clause no. 9.6, you have asked for "The proposed solution should allow exporting of reports in PDF, Excel(optional) and CSV format" - Nowadays in enterprise level firewall normally reports are never to be in editable format, request you to ammend to be PDF or HTML format.

- Please refer point – M in above Corrigendum.

*** ***