

4th December, 2020

PO No.: IBL_CSC_IT Hardware_04122020

Ref No.: PR-0000286953-IB

Connectivity IT Solutions Pvt. Ltd.

No.606-608, Eco Star, Vishweshwar Nagar Road,
Goregaon East, Mumbai – 400063

Kind Attention: Ruchesh Bhanushali

Sub: CISCO E-Mail Gateway Security Solution

Dear Sir,

This is with reference to your proposal dated 06th November, 2020 and subsequent discussions on the same; we are pleased to place our order as under:-

SR. NO.	PART NUMBER	DESCRIPTION	SERVICE DURATION(Month)	QTY	AMOUNT (INR)
1	Cisco Email Security Solution (Product+support+subscription)	As per the detailed (Detailed BoQ attached below - Annexure A)	36	Detailed bifurcation in Annexure A(below)	Rs.2,60,00,000
2	Cisco Email Security & Email DLP - Implementation Charges as per SOW	Includes : Installation, Configuration , Policy Migration , Testing & Roll Out & Resource Cost for On-Site Support (6 Months) (Detailed SOW - ANNEXURE B)	NA	1	Rs.24,00,000
3	Sustenance support	24 x 7 Support Service (Remote Support) Includes : 24x 7 Monitoring , Response & Resolution of Issues Reported , Policy Management , Reporting & Coordinating L3 Escalation with Cisco, MPLS Termination & Remote Connectivity (As Per Annexure B)	36	1	Rs.54,00,000
TOTAL					Rs.3,38,00,000

Total Order Value: Rupees Three Crores Thirty Eight Lakhs Only.

TERMS & CONDITIONS:

1. Taxes: Extra as applicable

2. HSN/SAC Code: 9983

3. Payment terms:

- Product & inbuilt support charges (Rs.2.60 Crs) will payable 100% post Delivery.
- Implementation Charges Rs.24 Lakhs will payable 100% Post signoff by IT stake holder.
- Sustenance support will payable on yearly advance basis. (Rs.18 Lakhs Per year)

Ruchesh
4/12/20
4/12/20

Page 1 of 14

PNA House: Basement, 1st Floor, 3rd Floor & 4th Floor, PNA House, Plot No 57 & 57/1, Street No.17, MIDC, Andheri East, Mumbai - 400 093, Maharashtra, India. Tel.: +91 22 6106 9200

Registered Office: 2401 Gen. Thimmaya Road, Pune - 411 001, India
Tel.: +91 20 2634 3201 Fax: +91 20 2634 3241 Visit us at www.indusind.com
CIN: L65191PN1994PLC076333

4. Warranty Support Window :

- **Support SLA back to Back with OEM as part of 24x7x4 Support:**
 - a. Advanced Replacement parts delivered to the customer's site within four (4) hours of Cisco's diagnosis and determination of failed hardware, twenty-four (24) hours per day, seven (7) days per week, including Cisco observed holidays.
 - b. Cisco will use reasonable commercial efforts to provide Four-Hour Response for customer-site delivery of the replacement part from the time Cisco diagnoses the problem and determines that a replacement part is required."

5. AMC :

- 4th Year Onwards AMC : Works out 29% on Combined cost appliance having break-up as below -
- Appliance - H/W : 14%
- Software Subscription: 100 % (Rs.60.83 Lakhs)

6. Bill To Address: As Below:

- **DC Mumbai:** M/s. IndusInd Bank Ltd., C/o Tata Internet Services Limited, Nelco Compound, Behind Tata Technopolis, Knowledge Park, Chakala Andheri East, Mumbai 400059

7. Ship To Address: As Below:

- **DC Mumbai:** M/s. IndusInd Bank Ltd., C/o Tata Internet Services Limited, Nelco Compound, Behind Tata Technopolis, Knowledge Park, Chakala Andheri East, Mumbai 400059

8. IndusInd Bank GST No.:

- **DC Mumbai:** 27AAACI1314G1Z3

9. Invoice Submission: Digital Invoices to be emailed to invoicing@indusind.com along with a sign off from the respective Stakeholder (Senior Management).

10. TAT for Invoice Submission: Invoice to be submitted within 3 months from date of supply of goods or services rendered, failing which the invoice will not be considered for payment.

11. Upload on GST Portal: Invoices submitted to the Bank should get uploaded on the GSTN portal with the correct Invoice Number, Invoice Date and GST No. under B2B (Maintain accuracy in figures, words & special characters)

Parshuram
4/12/20

U. B. Rao
29/12/20

12. Error in GST upload: Incase there is a wrong upload of invoice number or invoice date / Error in quoting Bank GST Nos. / Non-deposit of Tax to Govt. treasury / Non filling of GSTR1, etc., Connectivity IT Solutions Pvt. Ltd., will have to reimburse to IndusInd Bank, the amount of GST Cenvat loss.

13. Other Terms: The defined Scope is as per the agreed proposal and Support SLA back to Back with OEM.

Kindly confirm receipt of this Purchase Order.

Thanking you,
Yours faithfully,


Vikas Dube
Head – Technology Management Group


Rashmi
4/12/20

PO No.: IBL_CSC_IT Hardware_04122020

Ref No.: PR-0000286953-IB

Annexure "A"

ANNEXURE A (Detailed Bill of Material)				
Line Number	Part Number	Description	Service Duration (Months)	Qty
1.0	EMAIL-SEC-SUB	Cisco Email Security XaaS Subscription	---	1
1.1	SVS-EMAIL-SUP-E	ENHANCED SUPPORT FOR EMAIL SECURITY	---	1
1.2	ESA-ESP-AT-LIC	Cisco Email, AMP, Threat Grid-Premium File Analysis License	---	45000
1.3	ESA-GSU-LIC	Cisco ESA Graymail Safe-unsubscribe License	---	45000
1.4	SMA-EMGT-LIC	SMA Centralized Email Management Reporting License	---	45000
2.0	ESA-C695-K9	ESA C695 Email Security Appliance	---	6
2.0.1	CON-SNTP-ESAC695K	SNTC-24X7X4 ESA C695 Email Security Appliance	36	6
2.1	CCS-PSU1-770AC	Cisco Content Sec AC Power Supply 770W for x95 appliance	---	12
2.2	SFS-250V-10A-ID	SFS Power Cord - 250V, 10A , India	---	12
2.3	SF-ESA-11.5.0-K9	ESA Async OS v11.5.0	---	6
2.4	CCS-HDD-600GB10K	Content Sec x95 600GB 12G SAS 10K RPM SFF HDD	---	48
2.5	CCS-TPM2-002	Cisco Content Security Trusted Platform Module TPM 2.0	---	6
2.6	CCS-CPU-6126D	Content Sec 2.6 GHz 6126/125W 12C/19.25MB Cache/DDR4 2666MHz	---	6
2.7	CCS-MEM-16GB	ContentSecx95 16GBDDR4-2666MHzRDIMM/PC4-19200/slrnk/x4/1.2v	---	12
2.8	CCS-MRAID-M5	Cisco Content Sec SAS Modular Raid Controller 2GB Cache	---	6
2.9	CCS-PCIE-IRJ45	Cisco Content Sec quad port 1G Copper PCI	---	6
2.10	CCS-MESSAGING-LIC	Cisco Content Security Messaging License	---	6
2.11	ESA-BOUNCE-LIC	ESA Bounce Verification License	---	6
3.0	SMA-M695-K9	SMA M695 Security Management Appliance	---	2

Rashmi
4/1/20

GPB
24/12/20

3.0.1	CON-SNTP-SMAM695K	SNTC-24X7X4 SMA M695 Security Management Appliance	36	2
3.1	SFS-250V-10A-ID	SFS Power Cord - 250V, 10A , India	---	4
3.2	SF-SMA-11.1.0-K9	SMA Async OS v11.1.x	---	2
3.3	CCS-PSU1-1050AC	Cisco Content Sec AC Power Supply 1050W for x95 Appliance	---	4
3.4	CCS-HDD-600GB10K	Content Sec x95 600GB 12G SAS 10K RPM SFF HDD	---	32
3.5	CCS-TPM2-002	Cisco Content Security Trusted Platform Module TPM 2.0	---	2
3.6	CCS-CPU-4110D	Content Sec 2.1 GHz 4110/85W 8C/11MB Cache/DDR4 2400MHz	---	4
3.7	CCS-MEM-16GB	ContentSecx95 16GBDDR4-2666MHzRDIMM/PC4-19200/slrnk/x4/1.2v	---	4
3.8	CCS-MRAID-M5HD	Cisco Content Sec SAS Modular Raid Controller 4GB Cache	---	2
3.9	CCS-MESSAGING-LIC	Cisco Content Security Messaging License	---	2
3.10	CCS-PCIE-IRJ45	Cisco Content Sec quad port 1G Copper PCI	---	2
3.11	CCS-PCI-1B-240M5	Riser 1B incl 3 PCIe slots (x8, x8, x8); all slots from CPU1	---	2

Parthiv
4/12/20

V. D.
24/12/20

ANNEXURE "B"

SOW Implementation & Sustenance Support

Objective: This documents outline the high level scope of work that vendor shall abide by to implement and manage Email Security Gateway & Email DLP solution. (Termed as ESG)

Brief Scope of Work:

1. Analyze policies and settings currently running in the present email security solution (including DLP)
2. Install and Configure New ESG in Cluster Mode and New Security Management Appliance
3. This cluster of New ESG will require SMTP Load balancer to balance the load between the appliances both at DC & DR
4. Integrate New ESG with Active Directory & Netcore LDAP
5. Optimize and migrate the current setting & Configuration on to New ESG Cluster
6. SIEM Integration: The New ESG send message to the syslog server over Port 514 (TCP/UDP). Vendor team shall assist Bank team for integration of ESG with SIEM
7. Vendor shall document and request the Administrator or equivalent rights for the Vendor Support resource needs before the migration of setup
8. Configuration & Sharing of DNS entries related to SPF / DKIM / DMARC & MX
9. Testing of email flow
10. Vendor team shall assist the Bank IT team on the migration of MX records for email security. Ensure smooth migration with no outage or disruption.
11. Integration of ESG with ARCOS (PIM)
12. Migrate exiting reports & enhance wherever needed ,Within the reporting features available with proposed ESG
13. Migrate all the Mail Filtering, Alerting Policies (including management of Quarantine mails).
14. Ensure all features available in ESG are demonstrated and deployed in bank environment

Overview about Important Email Security Policies:

Key Features and Importance of SPF, DKIM , DMARC

Accurate and effective email spam and virus filter

New Email ATP uses combination of various techniques to accurately identify spoofed email, such as:

- **SPF & SenderID:** Sender Policy Framework (SPF) is an email validation system, designed to prevent unwanted emails using a spoofing system. To check this common security problem, SPF going to verify the source IP of the email and compare it with a DNS txt record with a SPF content published by the Email domain owner. Since it was derived from SPF, Sender ID can also validate the MAIL FROM. This will

Rashmi
4/12/20

4/12/20

help to identify spoofed emails

- **DKIM:** DomainKeys Identified Mail (DKIM), is a method to associate the domain name and the email, where the unique Mail server identifier is published as the DKIM signature.
- **DMARC:** Domain-based Message Authentication, Reporting & Conformance (DMARC) is a technical specification created by a combination of SPF and DKIM, which will help reduce the potential for email-based abuse by referring both the parameters in the DMARC of the sending email domain. DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms. The policy can be defined by the organization to Quarantine or Reject based on the parameter returned by the SPF and SKIM lookup.
- **rDNS:** The reverse DNS (rDNS) resolution is a determination of the domain name that is associated to an IP. Some email companies like AOL, for example, will reject any email that doesn't have a valid rDNS.
- **Boundary TLS Encryption:** Email encryption allows organizations to protect sensitive messages and increase their compliance with privacy regulations. One common encryption method, known as opportunistic TLS, automatically tries to secure the path that messages take when they travel to recipient email systems. Email ATP supports opportunistic TLS both for Inbound & Outbound email delivery.
- **Zero Hour Protection:** A New Virus Outbreak Filters provide a critical first layer of defense against new outbreaks hours before signatures used by traditional anti-virus solutions are in place. Real world results show an average lead time over reactive anti-virus solution of 13 hours, along with an extremely high catch rate and near zero misclassifications.
- **Advance Malware Protection:** Email ATP with New Advanced Malware Protection. Featuring file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for the continuous analysis of threats, even after they have traversed the email gateway. Users can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly.
- **Business Email Compromise / Forge Email Detection – FED Engine:** Display-Name Spoofing, Typically, the forged address is owned by a fellow employee that the attack victim trusts. A particular category of spoofing, called whaling, involves a victim who is a high value target such as a CFO, CEO or CIO. This can be controlled via Email Impersonation where VIP Names are protected.
- **Phishing Email Protection:** Protection provides sender authentication and BEC detection capabilities.

Scorcher
4/12/20

LD
4/12/20

Detailed Scope of Work/Project Plan:

Following is the details Scope of Work highlighting the responsibilities of both the sides on the implementation phase

The below document will be converted in a Project Tracker during the implementation phase

Activity Responsibility	Project / Task	Description
	Phase 1	PRE-REQUISITES
BANK's IT	Pre-requisite	Provide list of all the domains for provisioning in New ESG portal
BANK's IT	Pre-requisite	List of all the routes per domain to relay clean emails
BANK's IT	Pre-requisite	List of domain/ Ips/ email addresses/ policies from Existing Service to New ESG
BANK's IT	Pre-requisite	List of TLS enforcement domains for business partners
BANK's IT	Pre-requisite	Access to MS Exchange / Microsoft Office 365 Portal for modification & rule creation to allow email flow only from ESG Gateways
BANK's IT	Pre-requisite	Need to open New Service URLs with BANK WebProxy for seamless access to New ESG Instance URLs like SpamQ, Admin Portal, etc...
BANK's IT	Pre-requisite	Active Directory Public IP and Service Account Information for User Verification
BANK's IT	Pre-requisite	Access to DNS CPanel to publish SPF, DKIM, MX Records, etc. if any
BANK's IT	Pre-requisite	List of Email Server Public Ips/ Hostname that will be specified for outbound via CES if any
	Phase 2	CONFIGURATION
Vendor	Configuration	Domain Provisioning in New Email Security Appliance to accept emails
Vendor		Add Mail Server Hostnames / Public IPs in New ESG Inbound Routes
Vendor / BANK's IT	Configuration	User Verification via Active Directory Server/Netcore LDAP
Vendor / BANK's IT		Get the Active Directory details

Signature
4/12/20

Signature
4/12/20

Vendor / BANK's IT		Need service account readily available to get the data from AD
Vendor / BANK's IT		Start the configuration of the AD lookup & do a test run
Vendor / BANK's IT		Cross Check the User reference in ESG
Vendor	Configuration	Global default Attachment size is 50 MB for both inbound & outbound
Vendor		modify message size limit to as per BANK policy
Vendor	Configuration	Setup Antivirus, Antispam, Antimalware & Outbreak Settings
Vendor		As per the best practice guide (sheet 3), setup the Antivirus & Antispam Detection Settings
Vendor		Configure tagging & other antispam/antivirus settings
Vendor		Add Quarantine & Setup Quarantine Settings
Vendor	Configuration	Adding existing Approved/Blocked list of Existing Service to New ESG
Vendor		Approved List (IP/Domain/Email Addresses) as provided in prerequisites by the BANK
Vendor		Blocked List (IP/Domain/Email Addresses) as provided in prerequisites by the BANK
Vendor	Configuration	Adding of existing Content Policies & Filter of Existing Service to New ESG
BANK's IT		In case of any new Content Filter policies to be created and apply
Vendor	Configuration	Enable TLS Boundary Encryption
Vendor		List of shared TLS Enforced Business Partners (if any shared from the prerequisites)
Vendor		Add the TLS domain under Business Partner
Vendor		Test TLS Handshake for the added TLS domains
BANK's IT		Mode the TLS enforcement to be enabled (inbound, outbound or bidirectional)
Vendor		Activate the TLS Enforcement for the Listed Business Partner domains
Vendor / BANK's IT	Configuration	Setup Email disclaimers (text/html) in New Cloud portal as per requirement of BANK's IT

Garshuni
4/12/20

U. Per.
4/12/20

Vendor / BANK's IT	Configuration	Enable Spam Quarantine
Vendor / BANK's IT	Configuration	Enable Spam Quarantine for End Users
BANK's IT	Configuration	Open New ESG Public Ips in MS Exchange / Microsoft Office 365
BANK's IT	Configuration	Create an inbound connector in MS-Office365/On Premise to accept emails from New ESG (May not be required as Hybrid email delivery is handled by MS Exchange)
BANK's IT	Configuration	Raise case with MS-TAC to have the New ESG Ips whitelisted to avoid gateway level throttling (May not be required as Hybrid email delivery is handled by MS Exchange)
Vendor	Configuration	Specify Outbound IP's of BANK in New ESG
Vendor		Add the Outgoing IP's shared by BANK in New ESG Portal in outbound routes
-	Phase 3	TESTING
Vendor	Testing	Telnet validation test for Inbound IPs / Hostnames
Vendor		Telnet validation checks will be carried out on Incoming Routes (to Mail Servers)
Vendor		Share the test results to BANK for cross verification
BANK's IT		In case of any change required in Incoming routes
Vendor / BANK's IT	Testing	Validate Inbound Mail flow testing using ESG MX Records
Vendor	Testing	Validation check will be conducted for those IP sets
Vendor		Share the test results to BANK's IT for cross verification
BANK's IT		In case of any change required in Outbound routes
Vendor / BANK's IT	Testing	Test Outbound Mail Flow
-	Phase 4	MIGRATION & GO-LIVE
Vendor / BANK's IT	Migration	Additional MX pointing to New Email Security Appliance
Vendor / BANK's IT	Migration	Change MX weightage for email routing to New email Security Gateways (ESG)
Vendor / BANK's IT	Migration	Move the Outbound traffic via ESG phase wise for Email & Application Servers

Parshuram
4/12/20

U. D. S.
2/12/20

BANK's IT	Migration	Removing the old MX records (Existing Service) from DNS for all BANK migrated domains
BANK's IT	Migration	Removing the old entries are traces from Existing Service infrastructure
-	Phase 5	Monitoring & Operational
Vendor	Monitoring	Improvement using notification, rule base fine tuning, addition of rule bases, etc..
Vendor	Monitoring	Reduction in false positives and incident register in case of true positives
Vendor / BANK's IT	Monitoring	Overview of Reports
Vendor	Monitoring	Close observation on Quarantine, Reports and Message Tracking data
-	Phase 6	Ongoing Support & Maintenance
Vendor	Configuration	Improvement using notification, rule base fine tuning, addition of rule bases, etc.. (Change Management Process to be Followed)
BANK's IT	Configuration	Whitelist / Blacklist of Email Address, Domain or IP Address (to be followed via Change Management Process / Approval)
Vendor / BANK's IT	Support & Maintenance	Review of Reports with Bank (Weekly / Monthly / Quarterly)
Vendor / BANK's IT	Support & Maintenance	Close observation on Quarantine, Reports and Message Tracking data
Vendor	Support & Maintenance	Share Upgrade Plan with Bank IT team with Known Bug Fixes and new Features
Vendor	Configuration	Vendor to carry out upgrade (based on bank's timeline)

Rashid
4/12/20

U. Khan
28/12/20

Data Leakage Prevention:

Bank has Mail DLP solution implemented at present. By implementing the ESG, all such DLP policies shall be migrated and configured into the new ESG.

All such policies shall be tested being operationally successful.

All DLP incidents should be configured to be reported via at least email to concerned stake holders as prescribed by bank

Any new policy to be configured, old policy modification/deletion should be part of regular operational activity with no separate charges to bank.

Support Services Levels

Vendor will be responsible for maintenance and management of installed New Email Security setup & shall address all the issues / trouble tickets raised by customer

Bank on time to time basis will share the RBI Compliance Guide lines so as to adhere the same in context of Email Security.

Technical Support and Issue Response

1. Vendor will support on a twenty-four (24) hours/day by seven (7) days/week basis. Vendor shall assign dedicated technical account manager for level 3 escalations. Such manager shall be available 24x7 on call in case of exigency.
2. Provide technical support to the Bank for problems with the service and Liaise with the Bank to resolve such problems.
3. Whenever a Bank raises a problem, fault or request, for service information via support desk ticketing system , telephone or email or with Vendor , its priority level is determined and it is responded to as defined in the table below:

Santhosh
4/12/20

Santhosh
4/12/20

Priority Level	Definition	Response Target	Resolution Time
Critical	Loss of service that cannot be circumvented	Support Tickets to be responded within 30 Min	ASAP Best Effort
Major	Partial Loss of Service or service impairment	Support Tickets to be responded within 1 hour	ASAP Best Effort
Minor	Potential service affection to only a particular user or a set of users	Support Tickets to be responded within 4 hours	ASAP Best Effort
Request	Non-Service Affecting or Informative	Support Tickets to be responded within 12 hours	ASAP Best Effort
Question	Questions regarding the Service or features	Support Tickets to be responded within 24 hours	ASAP Best Effort

4. If in any calendar month Critical & Major Priority Level Tickets are not responded within the response target time period, the customer is entitled to the following service credits.

Percentage of Critical & Major Tickets not responded in committed time	Service Credits from Vendor
< 99 % but >=98.0%	1 Day Support Service Credit
< 98.0% but >=97.0%	3 Days Support Service Credit
< 97.0% but >=96.0%	5 Days Support Service Credit
< 96%	10 Days Support Service Credit

Perkins
4/12/20

APR
24/12/20

Important:

- **Right to Audit:** Bank has the right to audit vendor infrastructure at various locations via offshore or onsite visits. Also, bank may initiate such audit based on its own requirement or regulatory requirements. Such audits will not be limited to no. of instance during the year.
- **Security & Patching:** Vendor will be responsible to ensure all solution and devices/appliances under their management are patched to the latest version of security and product patches. Such solution devices/appliances are hardened and secured as OEM best practices and confirmations are shared with Bank team as per agreed scheduled and as per request basis.
- **Right to reject resource:** Bank has sole right to reject the resources (people) which it does not deemed fit to deliver services to bank. Bank will try to provide 30 days of notice to vendor on most cases. However, there may be instances (involving serious performance of confidentiality issues) where such resources would be removed from delivering service to bank with immediate effect post bank notice.
- **Acceptance of milestone for payments for services:** Bank has sole right on acceptance of milestone for services part of payment released to the partner. On completion of each milestone sign-off, Partner to raise invoice for the said service milestone which will be accepted by the bank. Partner and OEM of ESG Appliance shall ensure that all features committed are deployed to its 100% potential and are effective. Bank shall release full payment towards Hardware and Software Subscription within 30 days from the receipt of the Digitally Signed Softcopy Invoice.

Randhawa
4/12/20

1 Do
29/12/20