

10th July 2017

PO No: IBL_CSC_IT Hardware_032506
PR No: PR-0000135928-IB

Connectivity IT Solutions Pvt. Ltd.
No.606-608, Eco Star, Vishweshwar Nagar Road,
Goregaon East, Mumbai - 400 063

Sub: Procurement of Cisco 4110 & 4120 with Other Software

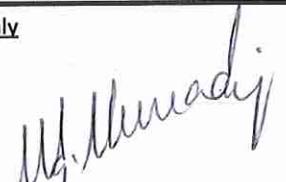
Dear Deepa,

This is with reference to your proposal No CS-SQ-2017-18/006 dated 4th July 2017 (Via Mail) and subsequent discussion on the same; we are pleased to place order as under:-

SL	P/N Number	HSN CODE	SAC CODE	Product Description - DC SIDE	UOM	Qty	Cost in INR
1	FPR4120-IPS + AMP-K9	8517.69.90		Cisco 4120 as NGIPS Appliance+ Advance Malware Protection in HA	Nos	2	
2	Interface Details	8517.69.90		8 * 1G Copper + 6 * 10G SR SFP with bypass enabled + 6 * 1G Copper with bypass enabled	Nos	Per Appliance	
3	L-FPR4120T-TM-3Y	RTU software subscription	998434	Cisco FPR4120 Threat Defense Threat (NGIPS) and AMP subscription for 3 Years	Nos	2	
4	Cisco Support & Hardware replacement	Support pack/AMC	998739	24X7X4 hours replacement support for 3 years	Nos	2	
5	Firesight Management	RTU software subscription		VM License for Centralised Management	Nos	1	
Total Product Cost- DC SIDE							24,453,006
998313							DC Solution - Implementation Cost 2,000,000
TOTAL DC COST							26,453,006

SL	P/N Number	HSN CODE	SAC CODE	Product Description - DR SIDE	UOM	Q 'ty	Cost in INR
1	FPR4110-IPS + AMP-K9	8517.69.90		Cisco 4110 as NGIPS Appliance+ Advance Malware Protection in HA	Nos	2	
2	Interface Details	8517.69.90		8 * 1G Copper + 6 * 10G SR SFP with bypass enabled + 6 * 1G Copper with bypass enabled	Nos	Per Appliance	
3	L-FPR4110T-TM-3Y	RTU software subscription	998434	Cisco FPR4110 Threat Defense Threat (NGIPS) and AMP subscription for 3 Years	Nos	2	
4	Cisco Support & Hardware replacement	Support pack/AMC	998739	24X7X4 hours replacement support for 3 years	Nos	2	
5	Firesight Management	RTU software subscription		VM License for Centralised Management	Nos	1	
Total Product Cost- DR SIDE							15,633,890
998313							DR Solution - Implementation Cost 1,000,000
TOTAL DR COST							16,633,890
TOTAL PRODUCT COST : DC + DR							40,086,896
TOTAL IMPLEMENTATION COST : DC+ DR							3,000,000
TOTAL SUSTENANCE COST FOR 1 YEAR							1,500,000
GRAND TOTAL COST (PRODUCT + IMPLEMENTATION+ SUSTENANCE)							44,586,896

Amount In Words: Four Crores Forty Five Lakhs Eighty Six Thousand Eight Hundred and Ninety Six Only



Page 1 of 7

IndusInd Bank Ltd., 4th Floor, PNA House, Plot No. 57 & 57/1, Street No.17,
MIDC, Andheri East, Mumbai, Maharashtra 400093, India. Tel: (022) 61069200

Registered Office: 2401 Gen. Thimmayya Road, Pune 411 001, India
Tel.: (020) 2634 3201 Fax: (020) 2634 3241 Visit us at www.indusind.com
CIN: L65191PN1994PLC076333



Terms & Conditions:

1. **Taxes:** 18% GST taxes extra as applicable at the time of billing.
2. **Annexure 1 – Detailed Bill Of Material**
3. **Annexure 2 –** Further to various correspondence Cisco and Connectivity Solutions are committed and accountable to deliverables as per Annexure 2.
4. Delivery 4-6 weeks from the date of PO.
5. **Warranty :** OEM Warranty with above mentioned support SLA
6. **Payment terms :**

Description	Milestone	Expected Due Date of Milestone
Product, License, Software & Cisco support	60% of the order value after delivery of materials	18 th August 2017
	40% post successful implementation	7 th November 2017
Implementation cost	100% Post Successful implementation	7 th November 2017
Sustenance cost	100% post implementation	7 th November 2017

7. In case of delay in implementation post 4 months from the date of PO, penalty of 5% of the implementation cost would be charged per fortnight.
8. Delays contributed due to any dependency on IndusInd Bank and/or beyond the control of vendor needs to be highlighted/escalated immediately and can be excluded mutually.
9. Formal trainings at least for 6 officials, since these are fairly new technologies.
10. **Freight:** Actual if the delivery locations are other than Bangalore, Delhi, Chennai & Mumbai, 0.5% of PO value. If the delivery locations are other than Bangalore, Delhi & Mumbai, Ahmedabad & Pune.
11. **Mode:** By Road, (By Air cost as per actual if required- on Request)
12. **Packing:** Extra, incase of special packing is required
13. **Insurance:** Our scope is up to the delivery address given in the PO. The same can be arranged & borne by customer incase delivery required other than PO address.
14. **Product Manuals:** Manuals are integrated with the electronic help system or as per OEM standard.
15. **Damage In transit:** All goods are insured in transit. CS/ Cisco Engineer shall inspect the goods immediately on arrival thereof in the presence of IndusInd Employee and check for any damage /loss in transit found in the goods and will, in case of any such damage/loss replace the same within 2 weeks from the date of original delivery.

16. Shipping Address:

DC: Tata Internet Building, 2nd Floor, Technopolis Knowledge Park, Nelco Compound, Mahakali, Andheri (East) Mumbai – 400 069

DR: Nxtra Datacenter, Plot F-08, Siruseri IT Park Sipcot, Chennai , Kancheepuram Dist. Tamil Nadu. 603103

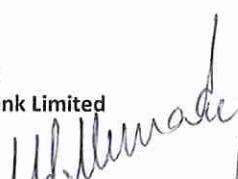
17. Billing Address: Mr. Shailesh Nanodkar, IndusInd Bank Ltd, PNA House, 4th Floor, Plot No. 57, Street No.17, MIDC, Andheri East, Mumbai – 400093. Contact No: 9833361312.

18. Cisco should ensure that solution proposed comply with our sizing requirement shared by our IT team. In case there is any performance gap due to undersized proposed solution, Cisco will provide higher end solution with no extra cost.

19. All other terms and further to various correspondence Cisco and Connectivity Solutions are committed and accountable to deliverables are as per the Proposal.

You are requested to acknowledge the acceptance of the above purchase order.

Yours faithfully
For IndusInd Bank Limited


Mohammed Mussadiq
Head- Technology Management Group

Annexure 1: Detailed BOM

Part Number	Description	Service Duration (Months)	Qty
Cisco NGFW 4100 firepower series with the hardware appliance and security features- DC location.			
FPR4120-BUN	Cisco Firepower 4120 Master Bundle	---	1
FPR4120-NGFW-K9	Cisco Firepower 4120 NGFW Appliance, 1U, 2 x NetMod Bays	---	2
CON-SNTP-FPR4121R	SNTC-24X7X4 Cisco Firepower 4120	36	2
FPR4K-NM-8X10G	Cisco FirePower 8 port SFP+ Network Module	---	2
CON-SNTP-F4KNMX1G	SNTC-24X7X4 Cisco FirePower 8 port SFP+ Network Modu	36	2
SFP-10G-SR	10GBASE-SR SFP Module	---	8
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	---	2
CAB-250V-10A-ID	AC Power Cord - 250V, 10A , India	---	4
SF-FXOS4K-2.0-K9	Firepower Extensible Operating System (FXOS) for FPR4K	---	2
SF-FPR-TD6.1-K9	Cisco Firepower Threat Defense software v6.1	---	2
FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	---	2
FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	---	2
FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit (Rack Mounts, Cables)	---	2
FPR4K-FAN	Firepower 4000 Series Fan	---	12
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	---	2
FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	---	2
GLC-T	1000BASE-T SFP	---	2
FPR4K-NM-8X10G	Cisco FirePower 8 port SFP+ Network Module	---	2
CON-SNTP-F4KNMX1G	SNTC-24X7X4 Cisco FirePower 8 port SFP+ Network Modu	36	2
SFP-10G-SR	10GBASE-SR SFP Module	---	16
L-FPR4120T-TM=	Cisco FPR4120 Threat Defense Threat and Malware License	---	2
L-FPR4120T-TM-3Y	Cisco FPR4120 Threat Defense Threat and Malware 3Y Subs	36	2
Cisco NGFW 4100 bundle with the hardware appliance and security features- DR location.			
FPR4110-BUN	Cisco Firepower 4110 Master Bundle	---	1
FPR4110-NGFW-K9	Cisco Firepower 4110 NGFW Appliance, 1U, 2 x NetMod Bays	---	2
CON-SNTP-FPR4110N	SNTC-24X7X4 Cisco Firepower 4110	36	2
SFP-10G-SR	10GBASE-SR SFP Module	---	16
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	---	2
CAB-250V-10A-ID	AC Power Cord - 250V, 10A , India	---	4
SF-FXOS4K-1.1-K9	Firepower Extensible Operating System (FXOS) for FPR4K	---	2
SF-FPR-TD6.0.1-K9	Cisco Firepower Threat Defense software v6.0.1	---	2
FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	---	2
FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	---	2
FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit (Rack Mounts, Cables)	---	2
FPR4K-FAN	Firepower 4000 Series Fan	---	12
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	---	2
FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	---	2
Cisco NGFW 4100 bundle with the hardware appliance and security features- DR location. Continue...			
GLC-T	1000BASE-T SFP	---	2
FPR4K-NM-8X10G	Cisco FirePower 8 port SFP+ Network Module	---	2
CON-SNTP-F4KNMX1G	SNTC-24X7X4 Cisco FirePower 8 port SFP+ Network Modu	36	2
FPR4K-NM-8X10G	Cisco FirePower 8 port SFP+ Network Module	---	2
CON-SNTP-F4KNMX1G	SNTC-24X7X4 Cisco FirePower 8 port SFP+ Network Modu	36	2

L-FPR4110T-TM=	Cisco FPR4110 Threat Defense Threat and Malware License	---	2
L-FPR4110T-TM-3Y	Cisco FPR4110 Threat Defense Threat and Malware 3Y Subs	36	2
	1G port SFP connectors - DC location.		
GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	---	24
	1G port SFP connectors - DR location.		
GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	---	32
	Cisco firesight management virtual appliance for centralized management of security features on 4100 platform - DC location.		
FS-VMW-SW-K9	Cisco Firepower Management Center, (VMWare) for 25 devices	---	1
CON-SAU-VMW	SW APP SUPP + UPGR Virtual FireSIGHT Software	36	1
	Cisco firesight management virtual appliance for centralized management of security features on 4100 platform - DR location.		
FS-VMW-SW-K9	Cisco Firepower Management Center, (VMWare) for 25 devices	---	1
CON-SAU-VMW	SW APP SUPP + UPGR Virtual FireSIGHT Software	36	1

Annexure 2:

Refer "Cisco and Connectivity Solutions" here as Vendor

Interfaces/Differentiators	Description	Vendor Commitment and Accountability
Hardware Interfaces	8 x 1G Copper + 6 x 10G SR SFP with bypass enabled + 6 x 1G Copper with bypass enabled for 3 years	4100 series appliances family has separate and different models namely 4110, 4120, 4140 and 4150. All these models are designed with fixed resources in terms of compute power configurations, however they offer modularity in terms of the kind of network modules that can be added for further expansion. The devices configured as per Bill Of Quantities BOQ have been fully populated with all available network module expansions.
Product features	Cisco Firepower Threat Defence (FTD) and Sourcefire integration new unified software.	Cisco acquired Sourcefire's FirePower a product series and Firepower Threat Defence (FTD) combines the firewalling features and traditional Sourcefire NGIPS capabilities for more enhanced performance and higher threat efficacies. Major deployment of New product 4100 FTD Series NGIPS with AMP which is built on SourceFire Platform client like TCS.
Product Features - Sandboxing	Cisco is not entirely dependent on the sandboxing driven approach	Out of 22K unknown files currently being noticed on daily basis only 2% would be going to our sandbox, which is a maximum of 440 files – rest will be analysed by on box AMP engine basis on our global threat intelligence (known as TALOS, which is included in the solution proposed) without relying on Sandbox. Cisco support maximum number of file types for sandbox and have no limitation of file size (allowed till 100 MB)
Product functions	Firepower Threat Defence (FTD)	FTD has been designed to provide all of the functions which were currently provided in NGFW, NGIPS and Anti-APT (AMP) solution perspective.



Interfaces/Differentiators	Description	Vendor Accountability/References																								
Product Testing	Product functionality testing and NSS LABS reports	Cisco FTD product is the best, futuristic and most threat-centric security platform that was built to date and as per NSS stringent and aggressive testing methodologies for both exploits as well evasion techniques Cisco FTD was still one the best performing platforms on Security Effectiveness.																								
	FTD 4110 has delivered only 25% of the claimed performance throughput only with HTTP (Non-SSL). NSS report state that "The Firepower 4110 is rated by NSS at 2,495 Mbps, which is lower than the vendor-claimed performance; Cisco rates this device at 10 Gbps."	Cisco performance testing shows higher performance based on typical traffic seen by a NGFW deployed to protect users. 4120 / 4140 / 4150 appliances are based upon SM36 / SM44 respectively and can achieve data sheet performance using single ports, whereas the 4110 (based upon SM24) needs 2 ports on each side of the test harness. NSS Uses only a single port in / out for throughput testing as a standard format of the testing process.																								
Product Market presence	Product FTD deployments - customer references	Large deployment in India - National Stock Exchange, TCS, National Informatics center																								
Sales and Support	Out of Sale & Out of Support date / year for proposed model	FTD- latest launch from Cisco with committed 7 years support.																								
Product performance throughput	I. 4110 & 4120 w.r.t. HTTP (Non SSL) & HTTPS (SSL) II. SSL throughput with TMC (IPS & APT) for 4110 & 4120.	I. Throughput for 4120 (Non SSL): 12 Gbps II. Throughput for 4120 (with SSL): 7 Gbps (Estimated) III. Throughput for 4110 (Non SSL): 7.8 Gbps IV. Throughput for 4110 (with SSL): 3.8 Gbps (Estimated)																								
Product SSL features	Number of SSL decrypted sessions supported simultaneously	I. For 4120: 5 Million II. For 4110: 3 Million																								
Product files Uploads	<table border="1"> <thead> <tr> <th>Features</th> <th>Bill Of Quantity</th> </tr> </thead> <tbody> <tr> <td>I.Threat Prevention Throughput (IPS + APT + URL)</td> <td>I. DC = 6.7 Gbps ; DR = 3 Gbps</td></tr> <tr> <td>II.SSL Inspection with IPS + APT + URL</td> <td>II. DC = 4 Gbps ; DR = 1.7 Gbps</td></tr> <tr> <td>III.29KB Transaction size for SSL</td> <td>III. SSL Inspection for 29 KB Transaction</td></tr> <tr> <td>IV.81 KB Transaction Size for Non-SSL</td> <td>IV. Non SSL Inspection for 81 KB Transaction</td></tr> <tr> <td>V.No of Files Uploaded for APT</td> <td>V. ~22000 files Daily</td></tr> </tbody> </table>	Features	Bill Of Quantity	I.Threat Prevention Throughput (IPS + APT + URL)	I. DC = 6.7 Gbps ; DR = 3 Gbps	II.SSL Inspection with IPS + APT + URL	II. DC = 4 Gbps ; DR = 1.7 Gbps	III.29KB Transaction size for SSL	III. SSL Inspection for 29 KB Transaction	IV.81 KB Transaction Size for Non-SSL	IV. Non SSL Inspection for 81 KB Transaction	V.No of Files Uploaded for APT	V. ~22000 files Daily	<table border="1"> <thead> <tr> <th>Cisco 4120 (DC)</th> <th>Cisco 4110 (DR)</th> </tr> </thead> <tbody> <tr> <td>I. 12</td> <td>7.8</td></tr> <tr> <td>II. 6.8</td> <td>3.8</td></tr> <tr> <td>III. N/A*</td> <td>N/A*</td></tr> <tr> <td>IV. N/A*</td> <td>N/A*</td></tr> <tr> <td>V. 1000 **</td> <td>1000 **</td></tr> </tbody> </table>	Cisco 4120 (DC)	Cisco 4110 (DR)	I. 12	7.8	II. 6.8	3.8	III. N/A*	N/A*	IV. N/A*	N/A*	V. 1000 **	1000 **
Features	Bill Of Quantity																									
I.Threat Prevention Throughput (IPS + APT + URL)	I. DC = 6.7 Gbps ; DR = 3 Gbps																									
II.SSL Inspection with IPS + APT + URL	II. DC = 4 Gbps ; DR = 1.7 Gbps																									
III.29KB Transaction size for SSL	III. SSL Inspection for 29 KB Transaction																									
IV.81 KB Transaction Size for Non-SSL	IV. Non SSL Inspection for 81 KB Transaction																									
V.No of Files Uploaded for APT	V. ~22000 files Daily																									
Cisco 4120 (DC)	Cisco 4110 (DR)																									
I. 12	7.8																									
II. 6.8	3.8																									
III. N/A*	N/A*																									
IV. N/A*	N/A*																									
V. 1000 **	1000 **																									
APT sandboxing analysis	Cisco assumption and reasoning of only 2% of the files will go to APT sandboxing analysis	Cisco count the files only on based on their unique SHA value, so if a file traverses through the AMP engine into the network with different names, types or polymorphs itself into different other files even for 1000 times, Cisco submission will still be counted as ONE because of a single unique SHA value, the file is queued for next cycle of submission without being dropped.																								



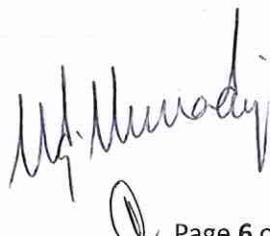
Interfaces/Differentiators	Description	Vendor Accountability/References
Product URL Filtering & End Point Posture Licensing/Impact	Licensing detail for URL filtering and end point posture as per proposed BOM.	<u>License requirement:</u> <ol style="list-style-type: none"> I. Not required for URL Filtering capability and can be added by adding URL's in block lists II. Required for category based URL blocking. III. Cisco FireSight Management IV. No separate End-point posture check licenses offered on NGFW/NGIPS from Cisco
	Impact of enabling SSL & URL filtering	Cisco commits no degradation of capacity of devices and Cisco standby with the throughput figures mentioned in the above <u>Product files Uploads description</u> table. Cisco completely take the ownership of either upgrading or adding new boxes to support the performance
	Cisco FTD 4120 performance impact from 12 Gbps to 3 Gbps.	Cisco stand by the commitment as stated above <u>Product files Uploads description</u> . SSL Throughput impact is estimated to be 50% for decryption (with current software based SSL decryption of 4100 series, however 4100 series is already being shipped with HW accelerators for SSL decryption which will be usable for deployments in next few releases). Once HW accelerators are activated the impact of SSL traffic (decryption) inspection is estimated to reduce to 25-30% only. Cisco device is done with 64 KB packet size, it will be much better than the performance numbers provided above <u>Product files Uploads description</u> .

Additional Information

NSS labs Security Value Map Competitive report for 2017.

Vendor	Security Effectiveness		Value (TCO per Protected Mbps)		Overall Rating
	25.8%	Below Average	US\$39	Below Average	
Barracuda Networks	89.6%	Above Average	US\$18	Above Average	Recommended
Check Point	95.5%	Above Average	US\$21	Above Average	Recommended
Cisco	99.9%	Above Average	US\$8	Above Average	Recommended
Forcepoint	78.6%	Above Average	US\$9	Above Average	Recommended
Fortinet 3200D	78.6%	Above Average	US\$5	Above Average	Recommended
Fortinet 600D	37.8%	Below Average	US\$105	Below Average	Caution
Juniper Networks	39.7%	Below Average	US\$20	Above Average	Caution
Palo Alto Networks	26.4%	Below Average	US\$39	Below Average	Caution
SonicWall	90.4%	Above Average	US\$6	Above Average	Recommended
WatchGuard	88.9%	Above Average	US\$8	Above Average	Recommended

Figure 2 – NSS Labs' 2017 Recommendations for Next Generation Firewall (NGFW)



Product	Exploit Block Rate	Evasions	Overall IPS Score
Barracuda Networks	95.6%	27%	25.8%
Check Point	99.6%	90%	89.6%
Cisco	95.5%	100%	95.5%
Forcepoint	99.9%	100%	99.9%
Fortinet 3200D	99.5%	79%	78.6%
Fortinet 600D	99.5%	79%	78.6%
Juniper Networks	97.0%	39%	37.8%
Palo Alto Networks	99.4%	40%	39.7%
SonicWall	97.9%	27%	26.4%
Sophos	96.2%	94%	90.4%
WatchGuard	98.7%	90%	88.9%

Figure 21 – Security Effectiveness (IPS)

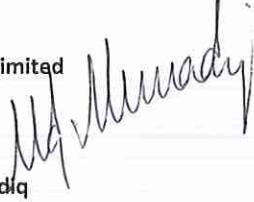
Figure 2 presents the overall results of the tests.

Product	Firewall	IPS	Stability and Reliability	Security Effectiveness
Barracuda Networks	100%	25.8%	100%	25.8%
Check Point	100%	89.6%	100%	89.6%
Cisco	100%	95.5%	100%	95.5%
Forcepoint	100%	99.9%	100%	99.9%
Fortinet 3200D	100%	78.6%	100%	78.6%
Fortinet 600D	100%	78.6%	100%	78.6%
Juniper Networks	100%	37.8%	100%	37.8%
Palo Alto Networks	100%	39.7%	100%	39.7%
SonicWall	100%	26.4%	100%	26.4%
Sophos	100%	90.4%	100%	90.4%
WatchGuard	100%	88.9%	100%	88.9%

Figure 2 – Security Effectiveness

You are requested to acknowledge the acceptance of the above purchase order.

Yours faithfully
For IndusInd Bank Limited



Mohammed Mussadiq
Head- Technology Management Group

