The Oriental Insurance Company Limited

Head Office, New Delhi

Corrigendum 1

For

Supply, Installation, Maintenance of Enterprise Backup Solution, Firewalls, Email Solution and Facility Management Services for Data Centers

(Tender Reference No.: OICL/HO/ITD/Tech-Refresh/2022/01 dated 21/09/2022)

Corrigendum dated 10/11/2022

Information Technology Department

The Oriental Insurance Company Limited
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

CIN- U66010DL1947GOI007158
www.orientalinsurance.org.in

1. Introduction

OICL has published the RFP vide tender No. OICL/HO/ITD/Tech-Refresh/2022/01 dated 21.09.2022 for Supply, Installation, Maintenance of Enterprise Backup Solution, Firewalls, Email Solution and Facility Management Services for Data Centers.

Following changes have been made in the above stated RFP. All other terms and conditions of the RFP shall remain unchanged. Please treat this Corrigendum as an integral part of the RFP documents issued.

Corrigendum

In reference to the aforesaid RFP, all are advised to note the following:

2. Modification in RFP Dates:

#	Page #	RFP Section	Original Date	Revised Date
1	-	Notice of Extension (ITD/HO/2022/L/ 691)	Last Date for Submission of Bids 14th November2022, 3:00 PM	Last Date for Submission of Bids 28th November2022, 3:00 PM
2	-	Notice of Extension (ITD/HO/2022/L/ 691)	Opening of Pre-Qualification bid 14th November2022, 3:30 PM	Opening of Pre-Qualification bid 28th November2022, 3:30 PM

3. Modification in RFP Clauses

#	Page #	RFP Section	Original Clause	Revised Clause
1.	16	1.6 Eligibility Criteria, Pt. 10	Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in last five (5) years. a) Enterprise class email solution for 4000 users using proposed email messaging solution in a BFSI/PSU/Government Organization in India b) Next Generation Firewalls in a BFSI/PSU/ Government Organization in India c) Enterprise class Backup Solution in a BFSI/PSU/Government Organization in India	Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in last five (5) years. a) Enterprise class email solution for 3000 users using proposed email messaging solution in a BFSI/PSU/Government Organization in India b) Next Generation Firewalls in a BFSI/PSU/ Government Organization in India c) Enterprise class Backup Solution in a BFSI/PSU/Government Organization in India

#	Page #	RFP Section	Original Clause	Revised Clause
			d) Should have maintained/ maintaining Facility Management Services for data center environment/ components such as network, compute, storage and security at DC and DR for at least one BFSI/ PSU/ Govt. Organization in India The cumulative order value for the above should be more than INR 25 crores	d) Should have maintained/ maintaining Facility Management Services for data center environment/ components such as network, compute, storage and security at DC and DR for at least one BFSI/ PSU/ Govt. Organization in India The cumulative order value for the above should be more than INR 25 crores
2.	18	1.7 Project Timelines, Backup	Installation, Configuration, Implementation & Integration Within 4 weeks from the date of delivery of backup suite	Installation, Configuration, Implementation & Integration Within 6 weeks from the date of delivery of backup suite
3.	21	2.2 Email Solution	Bidder is required to provide 11,000 email licenses & 11,000 email client licenses (including setup).	Bidder is required to provide 10,000 email licenses & 10,000 email client licenses (including setup). Rest of the details of Clause 2.2 remains same.
4.	22	2.2.3 Technical Requirements for Email Client	The email solution should support Mail clients through protocols viz. HTTPS, SMTP, MAPI & ActiveSync; Communications between mail clients and server through all protocols shall be encrypted and secure. Solution should run without enabling POP & IMAP protocols.	The email solution should support Mail clients through protocols viz. HTTPS, MAPI & ActiveSync; Communications between mail clients and server through all protocols shall be encrypted and secure. Solution should run without enabling POP & IMAP protocols.
5.	25	2.3 Email Security Solution	OICL is envisaged to procure and implement purpose built hardware appliance for on-premise email security solution including sandbox capability for their 8500 email users. The solution should meet all the requirements as per the Technical Specifications as mentioned under Appendix-1 in this RFP. Bidder to ensure that the Solution should have a Sender Policy Framework (SPF) designed to detect email spoofing by	OICL is envisaged to procure and implement purpose built hardware appliance for on-premise email security solution including sandbox capability for their 10000 email users. The solution should meet all the requirements as per the Technical Specifications as mentioned under Appendix-1 in this RFP. Bidder to ensure that the Solution should have a Sender Policy Framework (SPF) designed to detect email

#	Page #	RFP Section	Original Clause	Revised Clause
			providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. Also, MX, DKIM and DMARC (In-Bound) should be available in the Email Solution for all incoming mails.	spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. Also, MX, DKIM and DMARC (In-Bound) should be available in the Email Solution for all incoming mails. Rest of the details of Clause 2.3 remains same.
6.	42	3.1.6 Right to Alter Quantities	OICL reserves the right to alter the requirements specified in the tender. OICL also reserves the right to delete or increase one or more items from the list of items specified in the tender. OICL will inform the Bidder about changes, if any. In the event of any alteration in the quantities the price quoted by the Bidder against the item would be considered for such alteration. The Bidder agrees that the prices quoted for each line item & component is valid for period of contract and can be used by OICL for alteration in quantities. Bidder agrees that there is no limit on the quantities that can be altered under this contract. During the contract period the Bidder agrees to pass on the benefit of reduction in pricing for any additional items to be procured by OICL in the event the market prices / rate offered by the bidder are lower than what has been quoted by the Bidder as the part of commercial offer. Any price benefit in the products, licenses, software, services & equipment should be passed on to OICL within the contract period.	OICL reserves the right to alter the requirements specified in the tender. OICL also reserves the right to delete or increase one or more items from the list of items specified in the tender subject to a maximum of +-25%. OICL will inform the Bidder about changes, if any. In the event of any alteration in the quantities the price quoted by the Bidder against the item would be considered for such alteration. The Bidder agrees that the prices quoted for each line item & component is valid for period of contract and can be used by OICL for alteration in quantities.

#	Page #	RFP Section	Original Clause	Revised Clause
7.	50	4.26 Cancellation of the Contract & Compensation	OICL reserves the right to cancel the contract placed on the selected Bidder and recover expenditure incurred by the Company in the following circumstances: i. The selected Bidder commits a breach of any of the terms and conditions of the bid. ii. The selected Bidder goes in to liquidation voluntarily or otherwise. iii. The progress made by the selected Bidder is found to be unsatisfactory iv. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price. OICL reserves the right to cancel the AMC placed on the selected Bidder and recover AMC payment made by the Company, if the service provided by them is not satisfactory. In case the selected Bidder fails to deliver the quantity as stipulated in the delivery schedule, OICL reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility (capped at 5% differential value) of the selected Bidder. After the award of the contract, if the selected Bidder does not perform satisfactorily or delays execution of the contract, OICL reserves the right to get the balance contract executed by another party of its choice by giving thirty day's written notice for the same to Bidder. In this event, the selected Bidder is bound to make	OICL reserves the right to cancel the contract placed on the selected Bidder in the following circumstances: i. The selected Bidder commits a material breach of any of the terms and conditions of the bid. ii. The selected Bidder goes into liquidation voluntarily or otherwise. iii. The progress made by the selected Bidder is found to be unsatisfactory iv. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price. OICL reserves the right to cancel the AMC placed on the selected Bidder, if the service provided by them is not satisfactory. In case the selected Bidder fails to deliver the quantity as stipulated in the delivery schedule, OICL reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility (capped at 5% differential value) of the selected Bidder. After the award of the contract, if the selected Bidder does not perform satisfactorily or delays execution of the contract, OICL reserves the right to get the balance contract executed by another party of its choice by giving thirty day's written notice for the same to Bidder. In this event, the selected Bidder is bound to make good the additional expenditure (capped at 5%

#	Page #	RFP Section	Original Clause	Revised Clause
			good the additional expenditure (capped at 5% differential value), which OICL may have to incur in executing the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled. If the Contract is cancelled during AMC, OICL shall deduct payment on pro-rata basis for the unexpired period of the contract	differential value), which OICL may have to incur in executing the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled. If the Contract is cancelled during AMC, OICL shall deduct payment on pro-rata basis for the unexpired period of the contract
8.	-	Terms & Conditions, General	Addition to Terms & Conditions	**Transfer of Title** Title of ownership of goods supplied under this contract passed on to OICL on delivery of goods at the site
9.	58	6.4 Eligibility cum Technical Evaluation, Pt.4	Email Solution for 4000 users using proposed email messaging solution No. of Credentials: One BFSI/ PSU/ Government Organization in India Marks: 35 marks No. of Credentials: More than one BFSI/ PSU/ Government Organization in India Marks: 40 marks	Email Solution for 3000 users using proposed email messaging solution No. of Credentials: One BFSI/ PSU/ Government Organization in India Marks: 35 marks No. of Credentials: More than one BFSI/ PSU/ Government Organization in India Marks: 40 marks
10.	61	7 Service Level Agreement, 7.1.3 Availability	Availability of Equipment at DC & DR Penalty < 99.5 2% of the total cost of the FM for the year < 99.0 4% of the total cost of the FM for the year < 98.5 5% of the total cost of the FM for the year < 98.0	Availability of Equipment at DC & DR Penalty < 99.5 3% of the total cost of the FM for the quarter < 99.0 5% of the total cost of the FM for the quarter < 98.5 6% of the total cost of the FM for the quarter < 98.0

#	Page #	RFP Section	Original Clause	Revised Clause
			6% of the total cost of the FM for the year	7% of the total cost of the FM for the quarter
11.	94	Core Firewall, Pt. 1	The appliance based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one	The appliance based security platform should provide firewall, AVC, IPS and Antivirus functionality in a single appliance from day one
12.	94	Core Firewall, Pt. 6	Firewall should support at least 20,000,000 concurrent sessions or higher from Day 1	Firewall should support at least 10,000,000 concurrent sessions or higher from Day 1
13.	94	Core Firewall, Pt. 7	Firewall should support at least 600,000 connections per second	Firewall should support at least 500,000 connections per second
14.	94	Core Firewall, Pt. 12	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc.	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc and should support IPv6 features - NAT66, NAT46, NAT64, DNS64, DHCPv6 etc without any additional licenses
15.	94	Core Firewall, Pt. 23	The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box. The solution should support at least 15 Gbps or higher of SSL Inspection Throughput	The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box.
16.	96	Core Firewall, Pt. 34	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance	Clause stands deleted
17.	96	Core Firewall, Pt. 35	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download	Clause stands deleted

#	Page #	RFP Section	Original Clause	Revised Clause
			files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
18.	96	Core Firewall, Pt. 36	Proposed solution shall have required subscription like Threat Intelligence for proper functioning	Clause stands deleted
19.	96	Core Firewall, Pt. 37	Local Malware analysis appliance shall be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries or more in a virtual environment.	Clause stands deleted
20.	96	Core Firewall, Pt. 38	Local Malware analysis appliance shall have 20 VMs or more with relevant OS licenses along with integrated redundant power supply and minimum of 2 x 10 Gig ports or more	Clause stands deleted
21.	96	Core Firewall, Pt. 39	Should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Real time Attack footprint should be visible to the administrator for forensics purpose. Network-flood protection should include: • TCP floods, UDP floods & ICMP floods	Clause stands deleted
22.	96	Core Firewall, Pt. 42	The management appliance should have minimum 2 x 1G port and integrated redundant power supply from day one	The management appliance should have minimum 2 x 1G port and integrated redundant power supply from day one OR Management VM software should support minimum 2 x 1G port
23.	97	Core Firewall, Pt. 46	The management platform must provide centralized logging and reporting functionality with minimum 8TB of storage	The management platform must provide centralized logging and reporting functionality

#	Page #	RFP Section	Original Clause	Revised Clause
				with minimum 8TB inbuilt or through external storage solution
24.	97	Perimeter Firewall	Entire Specifications for Perimeter Firewall	Refer Section 4 of the Corrigendum for Revised Perimeter Firewall Specifications
25.	105	Email Security, Pt.9	The proposed solution Sandbox Language should support custom languages supported by Windows.	The proposed sandbox solution should support custom ISO images
26.	111	Backup Solution, Pt.21	Backup Solution should also have configurable REST API support for management, administration and reporting on backup infrastructure via custom applications and out of box integration with VMWare vRealize Automation for complete orchestration.	Backup Solution should also have configurable REST API support for management, administration and reporting on backup infrastructure via custom applications.
27.	112	Backup Appliance, Pt.1	Proposed purpose built backup appliance (PBBA) should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC , OST and NDMP protocols. All of the protocols should be available to use concurrently with global deduplication for data ingested across all of them.	Proposed purpose built backup appliance (PBBA) should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC , OST and NDMP protocols. All of the protocols should be available to use concurrently with deduplication for data ingested across all of them. Bidder to quote required capacity as per the sizing parameter mentioned in RFP in day 1. During the entire project period if any additional capacity required then bidder to provide it free of cost.
28.	113	Backup Appliance, Pt.6	Proposed purpose-built backup appliance (PBBA) should have the following capabilities such as replication, encryption, WORM, OST protocol, industry leading backup software integration.	Proposed purpose built backup appliance (PBBA) should have the following capabilities such as replication, encryption, WORM/Immutability, OST protocol, industry leading backup software integration.

#	Page #	RFP Section	Original Clause	Revised Clause
29.	113	Backup Appliance, Pt.10	Proposed purpose-built backup appliance (PBBA) should have the ability to perform different backup, restore, replication jobs simultaneously and must support communications and data transfers through 8/16 GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The Proposed backup appliance should be offered with min. 2 x 1Gbps NIC, 4 x 10Gbps NIC and 4 x 16Gbps FC ports.	Proposed purpose built backup appliance (PBBA) should have the ability to perform different backup, restore, replication jobs simultaneously and must support communications and data transfers through 8/16/32 GB SAN, 1/10/25 Gb & 1/10/25 Gb ethernet LAN over copper and SFP+. The Proposed backup appliance should be offered with min. 2 x 1Gbps NIC, 4 x 10/25Gbps NIC and 4 x 16/32Gbps FC ports.
30.	115	Backup Appliance, Pt.17	Proposed purpose-built backup appliance (PBBA) must have the capability for OST integration with NetBackup, Networker, Veeam etc.	Proposed back up software / appliance must have the capability for OST integration with at least three leading back up software's like NetBackup, Commvault, Veeam, Dell etc.
31.	115	Backup Appliance, Pt.18	Proposed purpose-built backup appliance (PBBA) should support retention lock (WORM) feature which ensures that no data is deleted accidently and support for point-in-time copies of a LUN or volumes with minimal performance impact.	Proposed purpose built backup appliance should support WORM /IMMUTABILITY feature which ensures that no data is deleted accidently even with admin/root access.
32.	115	Backup Appliance, Pt.19	Proposed purpose-built backup appliance (PBBA) should be offered with battery backed up RAM / NVRAM for protection against data loss in power failure scenario and continuous automated file system check to ensure data integrity.	Clause stands deleted
33.	115	Backup Appliance, Pt.24	Proposed purpose-built backup appliance (PBBA) should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user while maintaining a global deduplication across data from all tenant users.	Proposed purpose built backup appliance (PBBA) should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user while maintaining a global deduplication/ deduplication across data from all tenant users.
34.	115	Appendix 2: Commercial Bill of Material, Instructions;	Bidder is required to submit the indicative commercials during the bid submission and is	Clause stands deleted

#	Page #	RFP Section	Original Clause	Revised Clause
		Summary of Total Cost-Pt.15	required to provide the line item wise detailed breakup post reverse auction (RA)	

4. Specifications for Perimeter Firewall

#	Particulars
1.	Proposed firewall must be Enterprise grade Next Generation Firewall with complete threat prevention capabilities to improve the OICL Security Posture. The Next Generation Firewall appliance should be a purpose built appliance based solution with integrated functions like Firewall, IPSEC VPN, Application Awareness, IPS, BOT prevention, Antivirus and Zero Day Threat Prevention. **External and internal security system has to be from different OEM.**
2.	NGFW gateway architecture should have distributed architecture, whereby Management should handle Management functions like configuration, reporting, Logging etc. and strengthen security control to secure the confidential configuration of firewalls & Data should be processed by the Gateway according to NGTP configuration. Management and Firewall should be two separate systems. Management can be virtual appliance or bare metal hardware installation. SI has to provide the pre-requisites to implement the solution.
3.	Proposed gateway should be based on multicore architecture. All NGFW modules/features Firewall, Threat Prevention, VPN, SSL, URL must run on multicore architecture and not on ASIC from day1.
4.	The administrator must be able to view report on the CPU usage for management and Gateways separately.
5.	Proposed Gateway Appliance must have minimum of 64 GB or more of RAM.
6.	Proposed Solution must support VDOM/Multi-Instance/Virtual System/Multi Domain or equivalent architecture
7.	The device or any of its family should not have any feature of wireless within its hardware or software.
8.	Firewall should have integrated redundant hot-swappable power supply.
9.	Appliance should have 400+ GB SSD storage or more from day 1.
10.	NGFW must offer Min 8 x 100/1000 Copper interfaces from day one
11.	NGFW must offer 4x10Gig SFP/SFP+ ports with respective SR transceivers from Day 1 For HA communication the appliance should have 10G/40G interface to be used for connection synchronization.
12.	Appliance must have onboarded 10/100/1000Base-T OOB management and USB ports dedicated for console management. There shouldn't be any restriction to use dedicated HA ports.
13.	Minimum NG Threat prevention throughput in real world/Enterprise/Application Mix environment (by enabling and measured with Application-ID/App awareness, identity awareness, NGIPS, Anti-Virus, Anti-Spyware, content awareness, phishing, Anti Bot, URL filtering, zero day attack prevention and file blocking security threat prevention features and logging enabled should be 9 Gbps or more.

#	Particulars
14.	IPsec VPN throughput – 9 Gbps or more
15.	Proposed Gateway must support new sessions per second – Min 200,000 from day 1
16.	Proposed Gateway must support concurrent sessions – Min 2.5 million and scalable to cater additional users in future.
17.	The Proposed solution should support High Availability Configurations Active/ Passive or Active/Active Clustering
18.	The proposed Next Generation Firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3
19.	Solution must be able to segment the rule base in a layered structure for access control & threat prevention policies. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks. Support layer sharing within Threat Prevention policy.
20.	The proposed Next Generation Firewall shall have native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.
21.	The proposed Next Generation Firewall should have the ability to create custom application signatures and categories. Also the device should have capability to provide detailed information about dependent applications to securely enable an application
22.	The proposed Next Generation Firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP
23.	The proposed Next Generation Firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
24.	The Next Generation Firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment
25.	The Next Generation Firewall must have the capability to create DOS prevention policy to prevent against DOS attacks by defining the policy.
26.	NGFW must offer ability to enforce multiple apps on standard ports in a single rule.
27.	The NGFW should block the traffic based on geo location (country wise).The geo location-based configuration should be supported granularly for per policy and per application wise as per the business requirement.
28.	Proposed gateway appliance must support capability to process SSL decryption.
29.	Should have protocol decoder-based analysis which can statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits.

#	Particulars
30.	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.
31.	Should support more than 12,000 (excluding custom signatures) IPS signatures or more. It should support importing signatures from Third party tools, customizing IPS signature and creation of multiple IPS policy for different segments and zones.
32.	The proposed Next Generation Firewall shall perform content based signature matching and Anti-bot application must be able to detect and stop suspicious abnormal network behavior.
33.	The proposed Next Generation Firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour
34.	Should be able to perform Anti-virus scans for web & email protocols
35.	Solution should be capable of providing inline Zero-Day Phishing Prevention which should prevent access to phishing websites, both known and completely unknown, without the need to install and maintain clients on end-user devices. This gives OICL almost instant access to hosts target of phishing attempt for the investigation.
36.	Should be able to call 3rd party threat intelligence data to the Firewall policy in order to block those malicious attributes and such list should get updated dynamically with latest data.
37.	OICL should be able to add custom threat prevention signature in an automated way by converting Snort signatures into custom threat signatures.
38.	Solution must have automated correlation engine on the appliance and on centralized management tool both which can correlate a series of related threat events that, when combined, indicate a likely compromised event in OICL's network.
39.	The proposed Next Generation Firewall should have SSL decryption and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy).
40.	The proposed Next Generation Firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.
41.	The Next Generation Firewall supports TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring.
42.	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic
43.	The proposed Next Generation Firewall must be able to support Network Address Translation (NAT)
44.	The proposed Next Generation Firewall must be able to support Port Address Translation (PAT)
45.	The proposed Next Generation Firewall shall support Dual Stack IPv4 / IPv6
46.	Should support on Next Generation Firewall policy with User and Applications

#	Particulars
47.	Solution should provide IPv4 and IPv6, dual stack support from day one.
48.	The proposed Next Generation Firewall must support the following routing protocols: Static, RIP v2, OSPFv2/v3 , BGP
49.	The proposed solution must support Policy Based forwarding based on: - Interface - Source or Destination Address - Source or destination port - Services or ports
50.	The proposed solution should provide traffic prioritization QoS policy on a per rule basis: a. source address b. destination address c. port and services
51.	Proposed solution must support DHCP Client configuration & DHCP Server configuration.
52.	NGFW should support the following authentication protocols: LDAP, Radius, Kerberos .Solution must have inbuilt integration (AD/ LDAP) for Identity based policies. AD/LDAP integration shall work without any additional VM dependency.
53.	The proposed Next Generation Firewall's SSL VPN shall support the LDAP, Radius authentication protocols
54.	The NGFW must be able to acquire User Identities from: LDAP, Captive Portal, VPN, Terminal Services.
55.	OICL should be able to configure, manage and monitor NGFW using CLI and GUI both with central management solution.
56.	NGFW appliances must be managed from a centralized dedicated management system separate from the NGFW appliance
57.	Solution must support management of multiple security layers, providing superior policy efficiency and enabling you to manage security through a single pane of glass.
58.	Must provide dedicated centralized management for central configuration, provisioning, real-time monitoring, logging and customized reporting with the capability to create scheduled reports.
59.	NGFW management must provide functionality to automatically save policy version when a policy is pushed and must provide a option to revert back to previous state.
60.	Centralized management, reporting appliance can be physical or virtual form factor. If virtual, then all requisite licenses (like OS , DB ,any other software) has to be provided along with the solution. And Hardware requirement like VM infra will be provided by OICL. In case of Hardware appliance bidder need to propose management appliance considering High availability at both the locations DC,DR.
61.	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis.
62.	Should be able to create custom report base on custom query base any logging attributes.

#	Particulars
63.	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.
64.	OEM should be present in India from at least 5 years and should be proposed with 5 Years OEM support bundle with 24x7x365 days OEM direct TAC support, RMA unlimited software updates and subscription update support.
65.	The Bidder must include efforts to transform Layer 3/4 security policies from third-party firewalls to Layer 7 policies for enhancing OICL protection.
66.	The firewall hardware/operating system shall be tested and certified for EAL 4 / NDPP (Network Device Protection Profile)/ NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions and firewall must be ICSA certified.