OIL INDIA LIMITED
(A Government of India Enterprise)
P.O. Duliajan, Pin – 786602
Dist-Dibrugarh, Assam

CORRIGENDUM NO. 3 DATED 14.07.2023.

to

BID NO. GEM/2023/B/3600769 dated 22-06-2023.

For

Hiring of services for Integrated SD-WAN & FireWall solution for OIL, FHQ and all branch offices of OIL.

This Corrigendum is issued to notify the following changes:

1. The following Clauses stands amended/newly incorporated in REVISED 'Section-III Scope of Work (SOW)' as highlighted below:

Sl No.	Clause No.	Original Tender Clause	Modified/Newly incorporated Tender Clause
1.	Clause No. 2.2 Functional requirement Point No. 43	The SDWAN edge devices must work in HA (High Availability) mode in each location. To achieve this if L2 switch is required in between ISP, MPLS cloud and SDWAN devices, the bidder must provision the same in branch offices. For FHQ, Duliajan switches are not required. The minimum configuration of the switch is mentioned in Clause No. 2.3.	The SDWAN edge devices must work in HA (High Availability) mode in each location. To achieve this if L2 switch is required in between ISP, MPLS cloud and SDWAN devices, the bidder must provision the same. The minimum configuration of the switch is mentioned in Clause No. 2.3.
2.	Clause No. 2.3 Specification of NGFW & SDWAN edge device. **A. NGFW & SDWAN devices for FHQ, Duliajan: 2 Nos** Point No. 3	d) 04 (Four) numbers 10G SFP+ optical transceivers (Reach: 300m) must be supplied with each device from the same OEM.	d) 04 (Four) numbers 10G SFP+ optical transceivers (Single Mode, Reach: 300m) must be supplied with each device from the same OEM.

OIL INDIA LIMITED
(A Government of India Enterprise)
P.O. Duliajan, Pin – 786602
Dist-Dibrugarh, Assam

3.	Clause No. 2.3 **B. <u>NGFW & SDWAN devices for 11 Branch offices</u>:** Point No. 3	d) 04 (Four) numbers 10G SFP+ optical transceivers (Reach: 300m) must be supplied with each device from the same OEM.	d) 04 (Four) numbers 10G SFP+ optical transceivers (Single Mode, Reach: 300m) must be supplied with each device from the same OEM.

All others terms and conditions of the Bid Document remain unchanged. Details can be viewed at www.oil-india.com.

SECTION-III

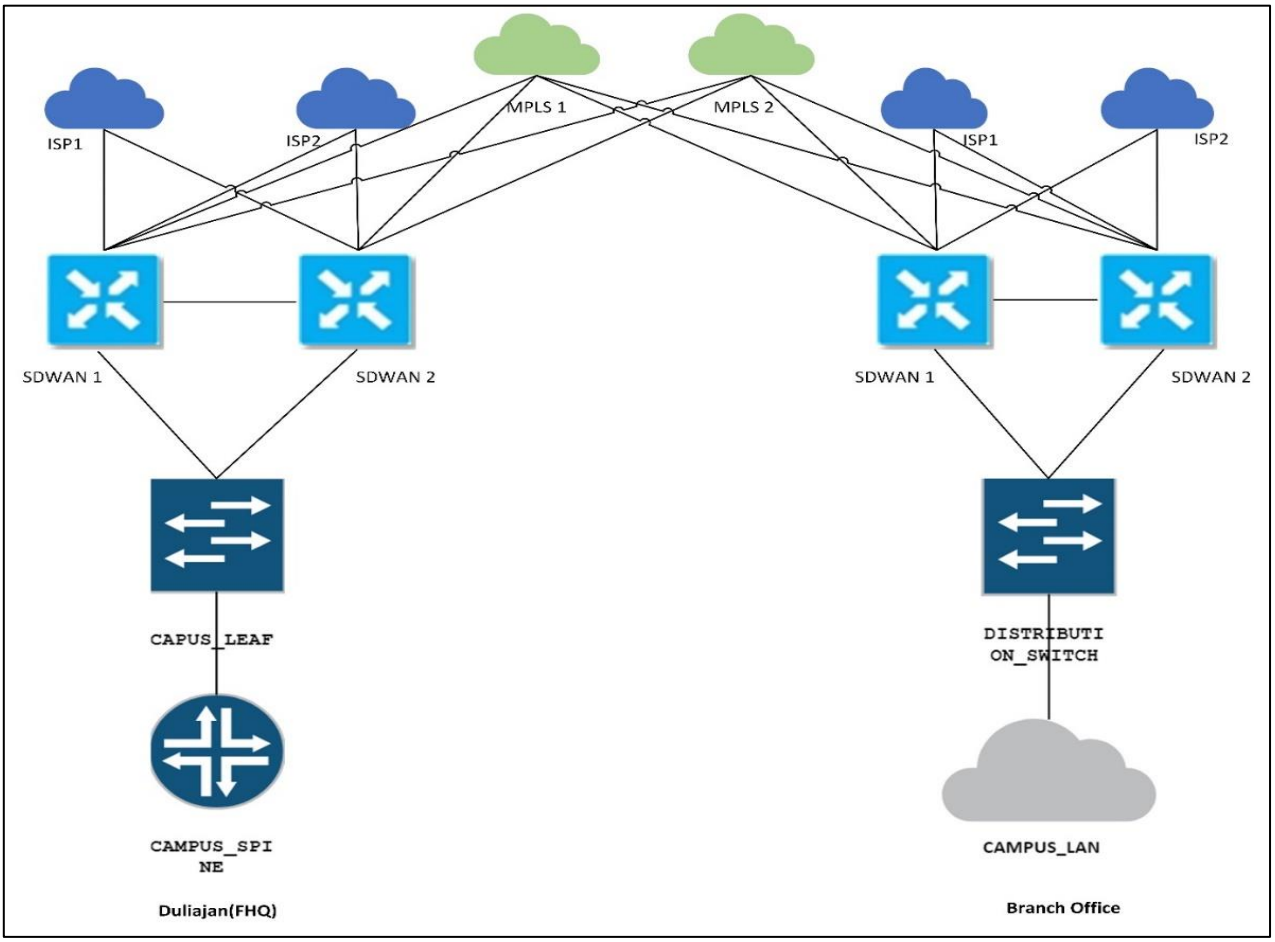
REVISED SCOPE OF WORK (SOW)

1.0 SCOPE OF WORK

Integrated NGFW (Next Generation FireWall) & SDWAN {Software Defined WAN (Wide Area Network)} solution for OIL.

OIL is currently having 02 (Two) nos. MPLS (Multiprotocol Label Switching) links and 03 (Three) nos. ILL (Internet Leased Line) links in FHQ-Duliajan Assam, office and 02 (Two) nos. MPLS links and 02 (Two) nos. ILL links in 11 other branch offices. OIL is planning to implement a SDWAN {**Software Defined WAN (Wide Area Network)**} solution with NGFW (**Next Generation FireWall)** capability built-in in SDWAN devices in FHQ Duliajan and 11 branch offices on OPEX (Operational Expenditure)/Rental model.

The proposed high level topological architecture of the solution is given below:



1.1 **Under this Contract, the Contractor shall be responsible for the following:**

1. Delivery & setup of integrated NGFW & SDWAN solution for all offices of OIL on rental basis.
2. Installation and Commissioning.
3. Training and solution documentation.
4. Managed Services for the entire solution for a period of 05 (Five) years.

1.2 OIL's current WAN infrastructure is as below:

Location of Primary Data center	Field Headquarters, Duliajan, Assam
Location of Disaster recovery site	Corporate Headquarters, Noida, UP
OIL offices and their locations	**Location**
Duliajan ,FHQ Digboi, FHQ	01 01
Guwahati, Assam	02
Kolkata, West Bengal	02
NCR 2 in Noida, UP 1 in Okhla, Delhi	03 (Including Director's office)
Jodhpur, Rajasthan	01
Kakinada, Andhra Pradesh	01
Bhubaneswar, Odisha	01
Type of MPLS Connectivity	MPLS (L3VPN) connectivity at all offices from BSNL & Sify. Currently OIL is using CISCO (Computer Information System Company) IWAN (Intelligent WAN) solution for MPLS connectivity across locations.
Internet connectivity	Direct Internet connectivity in all branch locations from BSNL & Sify.

1.3 Minimum Capacity of proposed solution:

The following table specifies the minimum required capacity to be provided by the solution from Day-1. The bidder must appropriately do the sizing of the offered components in the solution accordingly.

		Bandwidth					Number of Optimized Connections	Aggregate Throughput per Edge device
		MPLS-1	**MPLS-2**	**ILL-1**	**ILL-2**	**ILL-3**		
Primary WAN Aggregation Site: DULIAJAN	2000	200 Mbps	200 Mbps	500 Mbps	500 Mbps	Currently 48 Mbps Proposed is 500 Mbps	10000	4 Gbps
OIL House, Noida: NOIDA	250	200 Mbps	200 Mbps	200 Mbps	200 Mbps	NA	5000	2 Gbps
Noida (Director's Office)	50	NA	NA	200 Mbps	200 Mbps	NA	1000	2 Gbps
E&D office at Okhla	100	50 Mbps	50 Mbps	100 Mbps	100 Mbps	NA	1000	2 Gbps
PHQ, Guwahati	250	20 Mbps	20 Mbps	200 Mbps	200 Mbps	NA	2000	2 Gbps
Corporate Office, Guwahati	100	20 Mbps	20 Mbps	100 Mbps	100 Mbps	NA	1000	2 Gbps
COEES OIL,NRL building	250	20 Mbps	20 Mbps	100 Mbps	100 Mbps	NA	2000	2 Gbps
Kolkata Main office	250	20 Mbps	20 Mbps	100 Mbps	100 Mbps	NA	2000	2 Gbps
Kolkata Shipping office	100	20 Mbps	20 Mbps	50 Mbps	50 Mbps	NA	1000	2 Gbps
BEP office, Bhubaneswar	50	20 Mbps	20 Mbps	50 Mbps	50 Mbps	NA	1000	2 Gbps
Jodhpur office	250	20 Mbps	20 Mbps	100 Mbps	100 Mbps	NA	2000	2 Gbps
Kakinada office	100	20 Mbps	20 Mbps	100 Mbps	100 Mbps	NA	1000	2 Gbps

2.0 Scope of NGFW (Next Generation FireWall) & SDWAN {Software Defined WAN (Wide Area Network)} Solution:

The integrated solution shall have NGFW and SD-WAN capabilities as per the trailing functional specifications. One set of devices shall be installed in every office of OIL in high available manner. The Contractor shall design the appropriate topology and deployment architecture in consultation with OIL.

2.1 Architecture

The basic architectural model used in the proposed solution must consist of following logical components. Following is an indicative architecture and may change during implementation:

1. **Controller Device**: This device makes path optimization decisions and configuration of application-based forwarding policy and security rules are done on this device.

a. All policy and security rule configurations are done at the Controller device. The Contractor may offer the controller capability/services from OIL's data centre in Duliajan, Assam with their own devices or from any cloud data centre geographically located within India.

The Controller must be configured in HA (High Availability) mode.

b. Controller devices make path optimization decision for the respective sites and receives policy configurations from the Controller device.

2. **WAN Edge Device:** This is the device where WAN interfaces terminate. Edge device in each site make dynamic fully meshed encrypted overlay paths to every other edge device. This device forwards traffic to other branches over WAN including direct Internet access.

3. **Centralized Network Management & Monitoring:** This device provides comprehensive solution to manage, visualize, provision, automate configuration and monitor the proposed SD-WAN infrastructure from a single graphical interface. The Contractor may offer the monitoring capability/services from OIL's data centre in Duliajan, Assam with their own devices or from any cloud data centre geographically located within India.

2.2 **Functional requirement**

1. Each edge device must dynamically establish fully meshed encrypted overlay paths to every other edge device, across multiple different WAN services: L3VPN MPLS & Internet.

2. Each edge device must be able to do BGP (Border Gateway Protocol) peering with ISP (Internet Service Provider) routers for both MPLS and ILL.

3. The devices must support NAT (Network Address Translation).

- Source NAT with PAT (Port Address Translation)
- Static NAT
- Destination NAT with PAT
- Persistent NAT, NAT64

4. The solution must support site-site remote routing via the primary WAN-aggregation site (hub-and-spoke model).

5. The solution must support dynamic optimal direct site-to-site remote routing (spoke-to-spoke model).

6. The overlay paths established amongst the edge devices must support:

a. Transport of multicast, and broadcast traffic
b. The ability to run routing protocols: OSPF v2 and v3, BGP for IPv4 and IPv6

7. The local users in each of the branch offices must be able to access Internet directly without going through the HO.

8. The solution must use Ethernet as standard media type for WAN transport.

9. Edge devices must be able to load-balance traffic across multiple WAN paths based on load balancing algorithms efficiently using all available WAN bandwidth.

10. Edge devices must be able to identify and classify applications, including application-encrypted traffic. Identification and classification of at least the following classes of application types must be supported by the solution:

    a. SAP ERP
    b. Active Directory/LDAP
    c. SMTP (Simple Mail Transfer Protocol)
    d. IP Voice Telephony
    e. Web traffic
    f. H.323
    g. SIP (Session Initiation Protocol)

11. The solution must be able to dynamically control data packet forwarding decisions by looking at application type, performance, policies, and path status.

12. The solution must be able to monitor the network performance - jitter, packet loss, and delay - and make decisions to forward critical applications over the best - performing path based on the defined application policy.

13. The solution must respond to measured performance changes (degradation) in addition to link and node state changes (up/down) and adjust application forwarding accordingly.

14. The solution must be able to prioritize real time traffic over other traffic.

15. The solution must provide application-specific acceleration capabilities that improve response times while reducing WAN bandwidth requirements.

16. The solution must have application awareness with capability of deep packet inspection of traffic in order to identify and monitor applications' performance to determine what traffic is running across the network in order to tune the network for business-critical services, resolve network problems and to help ensure that critical applications are properly prioritized across the network.

17. All remote-site traffic must be encrypted when transported over WAN transport links: MPLS, Internet and 3G/4G network protecting Data Confidentiality and Integrity.

18. The encryption must be done as per IPsec standards using AES (Advanced Encryption Standard) with 128-bit keys or higher coupled with Internet Key Exchange Version 2 (IKEv2).

19. The use of encryption should not limit the performance or availability of a remote-site applications and should be transparent to end users.

20. The solution must use Hardware based encryption only and must give IMIX Encryption throughput equal to or greater than the sum total of WAN bandwidth capacity per site.

21. The solution must support zone-based firewall and VRFs to allow for network isolation.

22. The solution must have DoS/DDoS protection.

23. The Centralized management appliance must provide a single, unified platform for network service provisioning, monitoring and assurance and change management. The centralized management appliance must have web-based GUI (Graphical User Interface).

24. The solution must support zero-touch provisioning/plug-n-play for new branches, which entails on-site branch personnel having to make physical (i.e., cabling) changes only and administrators not having to make configuration changes to bring new branches online.

25. The solution must provide guided workflows for deployment and management of SD-WAN infrastructure.

26. The solution must support end-to-end real-time flow visualization for the application paths for identifying issues and taking corrective actions.

27. All network-wide configuration shall be from the centralized management appliance.

28. All application forwarding policies shall be configured from the centralized management appliance.

29. All NGFW policies shall be configured from the centralized management appliance.

30. The Central Unified Management must support management of at least 25 SD WAN devices with NGFW built in.

31. The Central Unified Management must support centralized logging for all the devices in the solution. The device must be able to collect logs of all events and policies from all the SD WAN devices in the solution.

32. The Central Unified Management must support forwarding of collected logs to an external syslog server.

33. The Central Unified Management must be able to analyse and correlate security logs and events in real-time for threat detection and automated alert notification for rapid response. The device must be able to automatically identify critical security events/compromises.

34. The Central Unified Management must be able to analyse and correlate historical log data.

35. The Central Unified Management must support drill-down of log data so that administrators can easily move from a high-level view to detailed analysis of events to follow the trail of an attacker and trace transactions.

36. Must support advanced report generation using the log data. Report generation must be possible on-demand and on a schedule with automated email notification.

37. The centralized management appliance shall have network, users, traffic and threat visibility for all the devices in the scope of the solution.

38. The solution must be able to collect and aggregate traffic statistics for all WAN paths. Traffic statistics include path utilization, application-specific utilization and path performance.

39. The solution must support device health monitoring for all the devices within the solution scope.

40. The solution must store historical traffic and performance information to assist with trouble analysis, traffic forecasting.

41. The solution must support syslog and email-based alarm to notify the administrators when any device/link fault or network performance degradation happens.

42. There should not be any dependency on the HUB site for inter branch office communication.

43. The SDWAN edge devices must work in HA (High Availability) mode in each location. To achieve this if L2 switch is required in between ISP, MPLS cloud and SDWAN devices, the bidder must provision the same. The minimum configuration of the switch is mentioned in Clause No. 2.3.

2.3 Specification of NGFW & SDWAN edge device.

A. <u>NGFW & SDWAN devices for FHQ, Duliajan: 2 Nos</u>

Hardware Specification	
1.	The bidder must specify the make and model of the quoted device.

	Make: Model:
2.	Form factor: Standard 19-inch rack mountable physical Hardware Appliance
3.	a) Minimum 08 (Eight) 1 GbE copper ports. b) Minimum 06 (Six) 1 GbE SFP port along with 6 x 1G SFP optical transceiver (Reach: 300 m) must be supplied with each device from the same OEM. c) 10G SFP+ ports: Minimum 04 (Four) numbers. d) d) 04 (Four) numbers 10G SFP+ optical transceivers (Single Mode, Reach: 300m) must be supplied with each device from the same OEM. e) Bidder must consider additional HA ports if required.
4.	Architecture: Control and data plane functionalities must have clear separation.
5.	Aggregate threat prevention throughput: Minimum 5.7 Gbps
6.	USB Port for external storage : Minimum 1
7.	Console port : Minimum 1
8.	Power supply : a) AC input voltage : 240 VAC b) AC input frequency : 50 Hz c) Redundancy: Power supply redundancy shall be provided from day-1 in such a way that there shall be no impact on services with fully loaded configuration (Hardware + Software) in case of single power supply failure.
9.	Encapsulations supported: a) Generic routing encapsulation (GRE) b) Ethernet c) 802.1q VLAN
10.	Cryptography support: a) Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes) b) Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit) c) Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512
11.	Protocol and Feature Support: a) IPv4 b) IPv6 c) Static Routes d) OSPF v2 and v3 e) BGP f) IKE g) VRRP h) ACL i) RADIUS j) AAA with TACAS+ k) NAT l) IEEE802.1ag m) IEEE802.3ah n) BFD o) VRF p) Hardware based IPsec VPN with capacity for minimum 100 tunnels

	q) LACP - 802.3ad
12.	Network Management support: a) SNMP V1/V2/V3 b) CLI access over Telnet and SSH c) GUI based configuration support d) Remote Monitoring support e) SYSLOG f) NetFlow or equivalent
13.	High availability Support: The device shall be configured in a manner to ensure that failure of one edge device does not affect the data forwarding as well as control path functionalities.
14.	The devices to have valid EAL certification.

B. NGFW & SDWAN devices for 11 Branch offices:

Guwahati - 2 (PHQ, NRL Building), Kolkata - 2, Bhubaneswar, Kakinada, Jodhpur, Noida Corporate Office, Noida Director Office, Okhla, Digboi

Hardware Specification	
1.	The bidder must specify the make and model of the quoted device. Make: Model:
2.	Form factor: Standard 19-inch rack mountable physical Hardware Appliance
3.	a) Minimum 08 (Eight) 1 GbE copper port. b) Minimum 06 (Six) 1 GbE SFP ports along with 6 x 1G SFP optical transceiver (Reach: 300m) must be supplied with each device from the same OEM. c) 10G SFP+ ports: Minimum 04 (Four) numbers d) 04 (Four) numbers 10G SFP+ optical transceivers (Single Mode, Reach: 300m) must be supplied with each device from the same OEM. e) Bidder must consider additional HA ports if required.
4.	Architecture: Control and data plane functionalities must have clear separation.
5.	Aggregate threat prevention throughput: Minimum 2.4 Gbps
6.	USB Port for external storage : Minimum 1
7.	Console port: Minimum 1
8.	Power supply: a) AC input voltage: 240 VAC b) AC input frequency: 50 Hz c) Redundancy: Power supply redundancy shall be provided from day-1 in such a way that there shall be no impact on services with fully loaded configuration (Hardware + Software) in case of single power supply failure.
9.	Encapsulations supported: a) Generic routing encapsulation (GRE) b) Ethernet

	c) 802.1q VLAN
10.	Cryptography support: a) Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes) b) Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit) c) Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512
11.	Protocol and Feature Support: a) IPv4 b) IPv6 c) Static Routes d) OSPF v2 and v3 e) BGP f) IKE g) VRRP h) ACL i) RADIUS j) AAA with TACAS+ k) NAT l) IEEE802.1ag m) IEEE802.3ah n) BFD o) VRF p) Hardware based IPsec VPN with capacity for minimum 100 tunnels r) LACP - 802.3ad
12.	Network Management support: a) SNMP V1/V2/V3 b) CLI access over Telnet and SSH c) GUI based configuration support d) Remote Monitoring support e) SYSLOG f) NetFlow or equivalent
13.	High availability Support: The device shall be configured in a manner to ensure that failure of one edge device does not affect the data forwarding as well as control path functionalities.
14.	The devices to have valid EAL certification.

C. L2 switch: 24 Nos

Hardware Specification	
1	Form factor: Height 1U (1.75 inch) max, mountable on wall, desk, rack with mounting kit. (Rack mounting kit to be supplied along with the device) LAN ports: Min 24 x 10/100/1000 Mbps Ethernet Uplink ports: a) Min 4 x 10GbE SFP+ b) Required 10 G SFPs (Single Mode) from same OEM supporting minimum 300 meter must be supplied along with the devices.

2	Switching Bandwidth (full-duplex capacity): Minimum 128 Gbps non-blocking switching capacity (Including stacking bandwidth)
3	Power Supply: 230V 50HZ AC (Indian Standard), Power Cable must be supplied.
4	Layer 2 feature: 802.1Q VLAN tagging with minimum number of VLAN supported: 1000 STP (802.1D), Rapid-Spanning Tree (802.1w), MSTP (802.1s) VTP/802.1ak or equivalent for registration/configuration of multiple VLANs LACP (IEEE 802.3ad) or equivalent for port-based redundancy LLDP (802.1AB), At least 1024 ARP entries.
5	Security features: IEEE 802.1x, RADIUS, TACACS+, Port-based (at least 256 ingress & 256 egress) & VLAN-based (at least 256 ingress & 256 egress) ACLs for IPv4 as well as IPv6 MAC based security on per port.
6	QoS: 802.1p QoS/CoS and Classification based on IP address, MAC address, VLAN, TCP/UDP port number. Management: SSHv2, as well as Web/HTTP/HTTPS (GUI) based management. SNMP v1, v2 and v3
7	Multi-Gigabit Support: No Console Port: Required
8	The switch to have valid EAL certification.

D. Functional built-in NGFW feature in the proposed solution:

Clause Number	Parameter	Specification
1.	Protocol Support	IP v4 and v6 dual stack , OSPF v1/v2/v3, BGP for IPv4 and IPv6
2.	Address Translation Support	a) Source NAT with Port Address Translation (PAT) b) Static NAT c) Destination NAT with PAT d) Persistent NAT, NAT64
3.	First Generation Firewall capabilities	a) Stateful Protocol Inspection b) Stateless Filters c) Zoning support d) Screening of DoS, DDoS, replay attack
4.	VPN Support	a) The firewall must support mobile access connectivity via remote access VPN to provide secure remote access to corporate resources from a wide variety of devices including smartphones, tablets, PCs, Mac and Linux. b) Minimum number of concurrent remote access VPN users via mobile access connectivity : 1800 c) Necessary licenses and client software to implement remote access VPN service via mobile access connectivity for at least 2000 users for the whole solution must be supplied

Clause Number	Parameter	Specification
		d) Minimum number of concurrent web based SSL VPN users: 200 e) Necessary licenses to implement web based SSL VPN service for at least 200 users for the whole solution must be supplied. f) Both client-based and web-based VPN connectivity must be supported. g) Both SSL and IPsec tunnel based remote access VPN connectivity must be supported. h) SSL VPN Portal: The firewall must support connecting securely to corporate resources through a portal from a web browser. Through an integrated Web portal, users must be able to access web applications, web-based resources, shared files, and email. The design of the web portal must be customizable. i) Authentication method supported - RADIUS, LDAP j) The VPN solution must support end user security posture checking of the endpoints before allowing them to connect to the OIL network. The necessary licenses and client software must be provided along with the solution for 1800 users. k) The VPN must have multi factor authentication support.
5.	Integrated signature based IPS (Intrusion Prevention System) support	a) It should be able to work with Vulnerability and exploit signatures and capable of Protocol anomaly detection and behavior-based detection. b) It should be able to provide real time protection based on daily and emergency IPS signature updates. c) It should be able to inspect SSL encrypted traffic. d) IPS engine must be integrated with the device not merely a co-located separate device. e) The bidder must give information on subscription model of IPS signature updates and provide updates as stipulated in the bid document.
6.	Application Awareness and control	a) It must be capable to identify, allow, block or limit usage (based on bandwidth and/or time) of standard applications, including Web 2.0 and social networking,

Clause Number	Parameter	Specification
		regardless of port, protocol or evasive technique used to traverse the network. b) It must be capable of SSL inspection and support TLS 1.3 c) It must have support for user role based policies i.e. application security based on user role and identity of all endpoints including mobile devices. d) The bidder must give information on subscription model of application classification signature updates and provide updates as stipulated in the bid document.
7.	Endpoint/User Identity Awareness	a) It must provide granular visibility of users, groups and machines, providing application and access control through the creation of accurate, identity-based policies. b) It must be able to integrate with Active Directory server for user identification.
8.	Web Content Filtering	a) It must be capable of web filtering based on categorized database b) It must be able to enforce inspection of all traffic, even when traversing non-standard ports and eliminate by-pass through external proxy c) It must be able filter SSL encrypted traffic d) The bidder must give information on subscription model of URL database updates and provide updates as stipulated in the bid document. e) Solution should be capable to use both signature based and ML based signature less technology. f) Should support DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs
9.	Anti-virus Capability	a) It must be able to block incoming malicious contents like : Virus, Trojans, Key logger etc. in real time based signature database b) The bidder must give information on subscription model of signature database

Clause Number	Parameter	Specification
		updates and provide updates as stipulated in the bid document
10.	Traffic Management and Quality of Service	a) It must be able to do QoS (Quality of Service) prioritization for both encrypted and unencrypted traffic. Application based QoS prioritization must be supported. b) It must support multiple ISP (Minimum two Internet Service Providers) redundancy support. It must be able to support internet access through multiple ISP links and able to switch over internet traffic to the working links when one or more ISP links fail. c) It must be able to distribute the internet traffic over multiple ISP links for load sharing.
11.	ATP-Protection against zero-day threats using cloud sandboxing	The firewall must be able to protect against zero-day threats using threat emulation technology like virtual "sandbox" environments. The Cloud based zero day threat protection must be supported. The firewall must be able to protect against Advanced Persistent threats like ransomware attacks and spear fishing.
12.	Updatable objects	The firewall must support updatable objects where in the objects are updated from APIs published by CSPs for e.g Microsoft publish their O365 IPs to be consumed by updatable objects of firewall which will be in turn used in firewall policies.
Administration and monitoring Features		
13.	Administration interface	It must support both GUI/Web and CLI (Command Line Interface) based user interface for administration and monitoring of the device.
14.		The firewall must be able to be managed locally and via Central Unified Management device offered as part of the solution. Using local management, the appliance should be able to manage itself.
15.	Monitoring	It must support real time network performance monitoring, sessions and bandwidth usage monitoring.
16.	Logging Support	It must support logging security events, user activity and system events. It must support analysis of the logs generated by allowing

Clause Number	Parameter	Specification
		search query and use of filters for different log types. Log size per day: The solution must be able to support minimum 2 GB of logs per day from each firewall. Log retention period: The solution must be able to retain logs in its own in-built storage for at least last 180 days.

3.0 Design of the Solution:

3.1 The Contractor shall design the solution as per OIL's requirement.

3.2 The design shall be done in the following 02 (Two) phases:

a) Phase-1 (Discovery and Assessment)
b) Phase-2 (Plan Development)

3.2.1 Following activities shall comprise Phase-1 (Discovery and Assessment)

a) Capture and review current network design, configurations, state, usage, connected endpoints, application attributes/behaviours etc.
b) Capture and review the current security policies and controls.
c) Collect and understand OIL's requirements. The findings of this phase shall be documented and submitted to OIL which shall serve as the baseline for migration activity.

3.2.2 Following activities shall comprise Phase-2 (Plan Development)

a) Create a detailed Method of Procedure (MOP) for all migration phases, including all device configurations, safe stopping points, verification checks, and rollback procedures.
b) The plan shall be designed to accelerate and optimize cutover times and mitigate migration-related risks.
c) The findings of this phase shall be documented and shall contain at least the followings:

i) High level design of the solution including the at least the following details:

- Traffic flows
- Network segmentation
- Security controls
- High availability and redundancy details
- QoS design
- Any change required in existing endpoints/network devices

ii) Detailed low-level design of the solution including at least the following:

- Physical topology with details of interconnected interfaces and endpoint connections
- Network Management platform
- The complete configuration of all the devices and components in the solution
- Firewall management component with policies and rules
- Any change required in existing endpoints/network devices
- User acceptance test (UAT) plan (covering all the technical requirements of the solution) to check and validate the solution post implementation.
- The documentation in this phase shall be submitted to OIL for approval.

4.0 Installation and Commissioning:

4.1 The team of installation engineers must be physically present at all sites during the installation and commissioning phase of the solution.

4.2 The Contractor shall be responsible for migration of existing firewall policies to the new firewall as per OIL's requirements.

4.3 The Contractor must provide documentation for installation and configuration after commissioning of the solution. The documentation must include step-by-step procedures to configure the devices.

4.4 The Contractor shall be responsible for any configuration changes required in the existing equipment like router, switches, firewall, servers etc. to integrate the solution with the existing infrastructure.

4.5 Cable dressing and management with tagging: The Contractor shall be responsible for cable dressing and management with tagging for all the interconnecting cables within the solution scope. Necessary Cable ties, cable channels and cable lacing cord, tag marker etc. must be supplied by the Contractor.

4.6 The Contractor shall ensure proper electrical earthing during physical installation of the equipment.

4.7 The UAT (User Acceptance Testing) shall be conducted by the Contractor in presence of OIL's personnel as per the UAT Plan. After successful completion of UAT, the Contractor shall submit detailed UAT report.

4.8 The installation and commissioning of the solution shall be deemed complete when all of the following requirements are met:

- Completion of delivery of all the items
- Set up of NGFW capabilities in the devices in all branches of OIL

- Set up of WAN comprising all branch offices with SD-WAN capabilities.
- Migration of around 200 FW policies from existing CheckPoint FireWall
- Set up of minimum 12 IP-Sec tunnels from IT data centre to various public clouds in line with the existing configuration in CheckPoint FireWall
- Completion of installation, configuration and integration for all the items
- Successful completion of User Acceptance Test
- Delivery of all the documentation
- Validation of the solution to ascertain that the implementation has been done as per the design document.

5.0 Training:

5.1 The Contractor must impart training to at least 08 (Eight) members of OIL's IT Personnel nominated by OIL. The training must be conducted in two batches. The training duration for each batch shall preferably be for a minimum 05 (Five) days.

5.2 The training content must at least include the following:

a) Basics of SDWAN technology
b) Features and capabilities of the supplied product
c) Administration and management of the supplied product
d) Troubleshooting and maintenance of the supplied product
e) Lab sessions

5.3 The bidder must arrange for necessary training infrastructure. The bidder is free to impart the training in any location of their choice in India. The training facility must be OEM authorized for imparting training on the offered solution. The training must be conducted by OEM certified instructor only.

5.4 Complete OEM published training material as per OEM curriculum must be provided either in hardcopy or softcopy to each participant. The training material provided must be standard course material provided as part of the course. The training material shall not be tailor-made for OIL.

5.5 Cost of transportation and accommodation of the OIL personnel for training shall be borne by OIL.

6.0 Managed Services:

6.1 The Contractor shall provide managed services for the SDWAN and NGFW solution valid for a period of 05 (Five) years from the date of completion of installation and commissioning for the solution.

6.2 All necessary tools, tackles and accessories required to manage the solution as per tender document shall be provided by the Contractor, at no extra cost to OIL.

6.3 The Contractor shall provide the details of escalation matrix for the Managed Services Operation.

6.4 The Contractor must have own relevant back-office infrastructure (tools and qualified human resources) to provide support for managed services operation. The Contractor shall not hire/outsource the required back-office capabilities from a third party bidder.

6.5 The Contractor must follow a documented change management process for any activity in any component of the solution.

6.6 There shall be a joint review meeting between OIL and the Contractor once every quarter to discuss issues, remedial actions, best practices pertaining to the solution.

6.7 The scope of the managed services shall include the following:

a) Rectification of any defects, faults and failures in the hardware and software components in the solution.
b) Preventive Maintenance: Physical Inspection, testing, satisfactory execution of all diagnostics, cleaning and removal of dust and dirt from the interior and exterior of the equipment, and necessary repair of the equipment at least once every quarter. Bidder's service engineer must visit each of the site to carry out this activity once in a quarter.
c) Health and performance monitoring of the solution: Continuous monitoring of the health and performance parameters of the solution and take necessary corrective actions.
d) Firewall log monitoring and security policy administration: Round the clock monitoring of the firewall logs and review and modification of security policies.
e) Any new configuration/modification of configuration to achieve any new requirement of OIL is in the scope of the bidder. The configuration related to establishing and monitoring new/existing IPSEC tunnel between OIL and CSPs is in the scope of the bidder.
f) Reporting: Submission of periodic report containing health and performance statistics of the solution, security events recorded in the Firewall logs and status of service requests for the week.
g) Investigation and analysis of security events recorded in the Firewall solution and recommendation of mitigation steps.
h) Supply and implementation of any firmware/Operating System Update/software update/Patch released by the OEM. Such updates must be provided free of cost.
i) Coordination with respective OEMs.
j) Backup and recovery management for the solution: Critical system files, configuration files or any necessary files which is needed to restore normal functionality of the solution in the event of any failure within the solution must be backed up. Necessary backup infrastructure will be provided by OIL.
k) Software License management for the solution.

l) Management/renewal of Content update/signature update subscriptions for the solution.

6.8 The managed services shall be governed by the following service level agreement (SLA):

a) All the activities in the scope of managed services shall be categorized into the following:

i) Service Request: Any operational/administrative job assigned to the managed service support by OIL as per the scope of the managed services for the solution.
ii) Software issue/Security Incidents recorded in the firewall: Any defect, fault, failure, performance degradation, and unavailability of services due to a software component in the solution; investigation and analysis, recommendation of mitigation step for any security events recorded in the Firewalls.
iii) Hardware issue: Any defect, fault, failure, performance degradation, unavailability of services due to a hardware component in the solution.

b) Service Delivery Requirement: The following table defines the service delivery requirement for the solution:

Category	Maximum resolution time
Service Request	8 hours
Software issue/Security incidents	12 hours
Hardware issue	120 hours

7.0 Other Terms and Conditions:

7.1 As a part of the project execution, bidder shall deploy the followings:

i) A dedicated design team comprising of qualified engineers with requisite skillsets in the direct payroll of the Contractor, for carrying out assigned tasks under design of the solution as per the scope of work in Para 3.0 above. This design team must include at least 01 (One) member with relevant professional level OEM certificate for the SDWAN devices. The bidder shall submit at the time of mobilization, the CVs of the members to be deployed during project execution.

ii) A dedicated installation and commissioning team led by at least 01 (One) installation engineer with relevant professional level OEM certificate for carrying out assigned tasks under the scope of work as per Para 4.0 above. In this regard, the bidder shall submit at the time of mobilization, the CVs of the proposed installation team attested by the CEO/Head of HR along with copies of relevant OEM certificate of the installation engineer.

iii) 01 resident engineer in FHQ Duliajan and 01 resident engineer in Noida, for managed services certified on the proposed OEM product. The resident engineers shall be provided necessary laptop, internet access etc. by the Contractor to carry out all operational activities for the project. In this regard, the bidder shall submit at the time of mobilization, the CVs of the members to be deployed.

7.2 The bidder shall have the following valid certifications:
a. ISO 20000-1:2011
b. ISO 27001:2013

7.3 The Contractor must supply the necessary software licenses and content update subscriptions to meet the stipulated specifications for a period of 05 (Five) years from the date of successful installation and commissioning of the solution.

7.4 The Contractor has to make his/her own arrangements for transportation and accommodation of its personnel when visiting various locations of OIL within the scope of the solution.

7.5 Pre-dispatch inspection at Seller premises:

Before dispatch, the goods may be inspected by OIL's representative at bidder's premises (or at designated place for inspection as declared/communicated by the seller) for their compliance to the NIT specifications. Two weeks of prior notice shall be given by Bidder to OIL so that necessary travel arrangements can be made; however OIL reserves the right to finalize the date for inspection. OIL shall bear the cost of travel and accommodation of OIL's representative for pre-dispatch inspection.

End of SOW