FTK - CENTER FOR INFORMATION TECHNOLOGY
Jamia Millia Islamia
(A Central University)
New Delhi - 110 025
Website: www.jmi.ac.in

E-TENDER FOR SUPPLY, INSTALLTION AND COMMISSIONING OF NEXT GENERATION FIREWALL/UTM FOR FTK– CENTER FOR INFORMATION TECHNOLOGY.

No. NIT-58/UTM/FIREWALL/CIT/JMI/2019-20-III Date: 03.10.2019

On behalf of the Vice-Chancellor, Jamia Millia Islamia (JMI), New Delhi, India, online bids (two bids system) are invited from reputed companies/firms for the Firewall with UTM Features (Appliance) for supply Installation and commissioning for Firewall/ UTM FTK-Center for Information Technology, Jamia Millia Islamia, New Delhi 110025. The order will be awarded for the period of five years & may be extended for on renewal basis, depending upon the performance and with mutual consent. Bid documents with other terms & conditions can be downloaded from Website: *https://eprocure.gov.in* and be uploaded along with notified EMD as per following:

EMD (Refundable)	Last Date & Time for online submission of bids	Venue for submission of EMD	Estimated cost in Rupees	Date/Time for opening of Technical Bid
Rs.3,20,000/-	23.10.2019 by 1.00 p.m.	Purchase & Inventory Control Office, Jamia Millia Islamia, New Delhi	Rs.160.00 lakhs	24.10.2019 at 3.00 p.m.
The Bid Security of the successful bidder would be returned, without any interest whatsoever, after the receipt of Performance Security from them as called for in the contract. EMD is not required to be submitted by those Bidders who are registered with the Central Purchase Organization (e.g. DGS&D), National Small Industries Corporation (NSIC). The EMD will be forfeited if the bidder withdraws or amends, impairs or derogates from the tender in any respect within the validity period of their tender.				

Minimum Warranty : Five Year
Website for Online bid Submission : https://eprocure.gov.in
Date/Time of Pre-Bid Meeting : 14.10.2019 at 11:00 Hrs
Last date & Time for online submission of bids : 23.10.2019 at 13:00 Hrs
Date/Time for opening of Technical bid : 24.10.2019 at 15:00 Hrs
Technical Specifications are available at the bottom of the document.

Tender is required to be uploaded in **two bids viz** 'Technical Bid' and 'Financial Bid' separately. Each and every page of the quotation is to be serially numbered and duly signed by authorized bidder/signatory. The rates should be written both in words and figures, free from erasing and over writing and error in typing/writing. Any erasing/error/ correction must be attested by the bidder otherwise the rates in r/o that particular item shall not be considered. Terms and conditions of the contract is enclosed as A**nnexure - 'A'** and format of undertaking is enclosed as A**nnexure - 'B'.** List of equipments is enclosed as **Annexure - 'C'**, Affidavit of criminal liability is enclosed as **Annexure- 'D'** and Details of the Service provider / Contractor is enclosed as **Annexure – 'E'.**

The Vice-Chancellor, Jamia Millia Islamia, JMI reserves the right to reject any tender or all without assigning any reason thereof.

Only technical bid (un-priced) shall be opened first and shall be referred for technical evaluation. The financial bid of only that technical bid which is found acceptable by the Technical Evaluation Committee will be considered for opening of Financial bids. The award of contract shall be considered to the lowest bidders fulfilling the conditions.

A) Technical bid:- Technical assessment will be evaluated on the basis of;

1. EMD in the form of D.D./ Bankers Cheque only in favour of Registrar, Jamia Milia Islamia, payable at New Delhi.
2. The firm must have similar experience of supply, installation & commissioning of network security equipment (Like Next Generation Firewall, UTM) for al least 1000 network nodes.
3. Bidder should submit at least three Order Copies as a token of proof of similar experience of networking security equipment along with completion certificate with details of customer name, concerned person contact number and e-mail id for verification purpose.
4. Undertaking as per **Annexure B.**
5. Manufacturer Authority letter from manufacturer / authorized service provider certificate in case bid is submitted by authorized agent / channel partner, without which bid will be summarily rejected.
6. Proposed BOQ/ Solution.

B) Financial Bid:- It should comprise the following:-

The information given in technical bid should be reproduced with prices against quoted equipment's. Any deviation in this regard will render the bid liable for rejection. The prices should be quoted on lump sum basis over and above with GST. All the rates shall remain firm for a period of 6 Month from the date of bidding.

Eligibility Criteria:

For Bidder

1. The Bidder should be an established Information Technology Private/Public company registered under Companies Act, 1956 or a registered firm. The company should have been in existence for more than 3 years as on date of opening of bid.

2. A letter of authorization from the Principal should be enclosed.

3. The bidder should be an authorized partner of the OEM. A copy of the agreement or authorization certificate in this regard has to be enclosed.

4. Financial: Turnover - Average Annual Turnover of the bidder during last three financial years, i.e., FY 2015-16, 2016-17, FY 2017-18 should be at least Rs. 3.20 Cr. - CA Certificate with CA‟s Registration Number/Seal.

5. The bidder should be a profit making organization in each of the last preceding 3 years.

6. The Bidder should not be currently blacklisted or have been blacklisted with any Government of India Agency/ PSU, any State Government department i. The bidder shall furnish a written declaration in this regards.

Proposed: BOQ / Solution.

S.No.	Description	Make/ Model	OEM Name	Quantity
1	**Next Generation Firewall / UTM Appliance.**			**2**
2	**Subscription & Support for Next Generation Firewall / all UTM features for 5 year.**			**2**
3	**Logging & Reporting Hardware Solution.**			**1**
4	**Advanced Add-on Network Security Feature for 5 year.**			**1**

Annexure – A

TERMS AND CONDITIONS:

1. All types of Spares and accessories should be available with the vender for quoted equipment's.
2. Support should be provided for 24 x 7 x 365 by OEM TAC support and advance Next Business Day Hardware replacement. All the updated should be provided free of cost for five years.
3. The bidder shall have to provide **Two** Regular preventive maintenance services in a year.
4. Firm has to provide warranty/guaranty on replaced spare for 5 (Five) Year minimum or as per the order placed.

14. Any act on the part of the contractor to influence anybody in the FTK-CIT, JMI shall make his tender liable for rejection.

16. **Performance Security deposit by the successful bidder will have to be deposited in the form of Demand Draft/Banker's Cheque/PBG for the amount decided at the rate of 5% of the order value of the contract amount in the favour of "Registrar, Jamia Millia Islamia", payable at New Delhi.**

17. **If any Tenderer fails to fulfill the above terms or violate any above terms his tender will be rejected summarily without assigning any reason or justifications**.

18. The quantity mentioned against each items in Annexure `C' is provisional and liable to change. However the exact quantity will be intimated at the time of award of contract.

19. Company/Service Provider should submit a letter mentioning the person deputed/ representative is authorized on behalf of Company/Service Provider stating the name of person, address and designation by competent authority.

Annexure – 'B'

Format of undertaking to be submitted along with tender for supply Installation and commissioning for NEXT GENERATION FIREWALL / UTM**.**

TO BE SUBMITTED ON A STAMP PAPER OF RS.100/- :

UNDERTAKING:

We hereby undertake that all the components/ parts/ assembly/ software used in the equipment shall be genuine, original and new components /parts/ assembly/ software from respective OEMs of the products and that no refurbished/ duplicate/ second hand components/ parts/ assembly/ software are being used or shall be used. In respect of licensed operating system, we undertake that the same shall be supplied along with the authorized license certificate with our name/logo. Also, that it shall be sourced from the authorized source for use in India.

In case, we are not found complying with above at the time of delivery or during installation, for the equipment already billed, we agree to take back the equipment already supplied at our cost and return any amount paid to us by you in this regard and that you will have the right to forfeit our Bid Security/SD/ PSD for this bid or debar/black list us or take suitable action against us.

Signature of Bidder

Name:

Address:

Contact No.

ANNEXURE C

FORMAT

PRICE BID SCHEDULE

1. Tender No:
2. Name of Supplier:

S.No.	Description	Make/ Model	Unit Price (in Rupees)	Qty	Total Price (in Rupees)	GST As Applicable	Total With GST
1	**Next Generation Firewall / UTM Appliance. (as per Specification)**			**2**			
2	**Subscription & Support for all UTM features for 5 year.**			**2**			
3	**Logging & Reporting Hardware Solution.**			**1**			
4	**Advanced Add-on Network Security Feature for 5 Years**			**1**			
	Total Amount						

Total Price In words:

Signature of Bidder

Name:

Address:

Contact No.

Annexure-D

AFFIDAVIT ON CRIMINAL LIABILITY

CRIMINAL LIABILITY UNDERTAKING ON RS. 10/- STAMP PAPER

I …… ……S/o Mr. …….. Resident of

(Address)……..

do solemnly pledge and affirm:-

1. That I am the proprietor/Partner/Director of the M/s……..

2. That no case of any nature i.e. CBI, Criminal/Income Tax/ Sales Tax/ Blacklisting is pending against the firm at the time of submission of Tender.

.

Signature of the Tenderer

Rubber Stamp of Tenderer

Mobile No……..

PAN No……..

E-mail ……..

Annexure-E

DETAILS OF THE SERVICE PROVIDER / CONTRACTOR

1. Name of proprietor / Authorised Signatory :
2. Name of the Participating Firm / Company :
3. Postal Address :
4. Telephone/Mobile No. :
5. Email :
6. Tin No. /GST :
7. Firm Registration No. :
   (if any)
8. NSIC / MSME Registration No. If any :
9. PAN No. :
   (Attach photocopy)
10. Name of the Directors/Partners/ Proprietor of the Firm/Company
11. Bank Account details for RTGS payment

    a) Beneficiary Name :
    b) Bank name & Branch Address :
    c) Account Number :
    d) IFSC :

(Signature with Seal)

SEQUENCE OF DOCUMENTS TO BE UPLOADED

Technical Bids and Financial bids are to be uploaded separately.

1. Forwarding letter duly signed by the Authorized person.
2. Balance sheet with auditor's report for the years 2015-16, 2016-17 & 2017-18.
3. GST Certificate
4. Proof of the authorized agent/distributors/supplier.
5. Sole Proprietary/sole manufacturer certificate for proprietary item.
6. Name and address of registered office, Head Office and Regional office of the company with name and phone numbers of key persons.
7. Format of Schedule of Requirements at Annexure-A
8. Undertaking at Annexure-B
9. Financial Bid at Annexure-C
10. Affidavit at Annexure-D
11. Details of the firm at Annexure-E
12. Proposed BOQ / Solution.

Note: Each document shall be duly signed and stamped by the vendor.

Scope of Work:

Migration of existing firewall to the proposed firewall solution as per the existing setup.
Successful bidder will be required to provide training to CIT Staff (firewall/network related staff) for administration/operation use at site.

Technical Specifications

GENERAL REQUIREMENTS OF INTERNET SECURITY SOLUTION AT JMI

1. The security platform should provide firewall, application visibility control and intruder protection services functionality in a single appliance from day one.
2. The proposed solution must be Easy to manage and operate by JMI CIT department.
3. Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc
4. Should support capability to integrate with other security solutions to receive contextual information like security group tags/names
5. Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
6. Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.
7. The solution must be able to detect & block advanced malware regardless of the specific ports or protocols used by the malware.
8. The solution must be able to detect and block malware using protocols different from HTTP/HTTPS.
9. The solution must be able to detect and block advanced malware used for both opportunistic attacks and targeted attacks targeted for this specific organisation.
10. The solution must be able to protect at least from the following categories of malware: botnets, exploit kits, drive-by, phishing.
11. The solution must be able to detect and block, suspicious DNS requests returning RFC1918 compliant IP addresses not allowed to be routed on the Internet, or directed to DNS services.
12. The solution must leverage predictive intelligence and not use static signatures or blacklists
13. The analysis algorithms must be enforce predictive detectors able to identify in real time, where attacks are staged and consequently predict and prevent the next move of attackers.
14. The threat intelligence must be automatically updated in less than 15 minutes after the discovery of a new threat without any manual update operations.
15. The solution must include a transparent intelligent proxy configurable inside each security policy and able to analyse both HTTP and HTTPS traffic.
16. The solution must have Ability to Enhanced visibility to the user internet activity by logging user email to the Internet logs
17. The solution must have Ability to Enforce policies to block in-appropriate content Management Requirements
18. The management interface must be web-based.
19. The management interface must provide a graphical policy editor to define security and web filtering policies.

TECHNICAL SPECIFICATIONS FOR NEXT GENERATION FIREWALL / UTM

Feature	Technical Specification	Compliance (Yes/No)
Industry recommendations	The Firewall solution offered must be rated as leaders in the latest Magic Quadrant Report for Enterprise Firewall published by Gartner	
Performance & Scalability	Should support 10 Gbps of Next Generation Firewall (Firewall, Application Visibility Control & Intruder Protection Services) real-world / production performance	
	Should support 12 Gbps of Application Throughput with 1024B packet size.	
	Firewall should support atleast 4,500,000 concurrent sessions with application visibility turned on	
	Firewall should support atleast 30,000 or higher connections per second with application visibility turned on	
	Firewall should have integrated redundant hot-swappable power supply	
	Firewall should have integrated redundant hot-swappable fan tray / modules	
Hardware Architecture	The appliance based security platform should provide firewall, application visibility control and intruder protection services functionality in a single appliance from day one	
	The appliance should support atleast 6 * 10G Gigabit ports and should be scalable to additional 8 * 10G Gigabit ports if required in future.	
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 64 GB of RAM	
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
	The proposed solution should not use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet.	
	Proposed firewall should not consume more than 2RU of rack space	
NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc	
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	

	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
	Should support Multicast protocols like IGMP, PIM, etc	
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness.	
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
	Should be capable of detecting and blocking IPv6 attacks.	
	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.	

	The solution must provide IP reputation feed that comprised regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. I	
	Should support Open based Applicaion ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
DNS Security	The solution must be able to protect at least from the following categories of malware: botnets, exploit kits, drive-by, phishing.	
	The solution must be able to detect and block advanced malware regardless of the specific ports or protocols used by the malware.	
	The solution must be able to detect and block malware using protocols different from HTTP/HTTPS.	
	The solution must be able to detect and block advanced malware used for both opportunistic attacks and targeted attacks targeted for this specific organisation.	
	Solution must have capability to block categories of applications and websites for proxies and anonymyzers.	
	Solution must support atleast 78 categories for filtering of web requests.	
	The solution must leverage predictive intelligence and not use static signatures or blacklists	

Anti-APT / Malware Features	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or file submission on cloud as they transit the network and capability to do dynamic analysis.	
	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 files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
Management	The solution should have separate management appliance for centralized management of Firewalls and Logging & Reporting.	
	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted	
	The management appliance should have 2 x 1G port and integrated redundant power supply from day one	
	The management platform must be able to store record of 30000 user or more	
	The management platform must provide a highly customizable dashboard.	
	The management platform must domain multi-domain management	
	The management platform must provide centralized logging and reporting functionality	
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
	Should support troubleshooting techniques like Packet tracer and capture	
	Should support REST API for monitoring and config programmability	
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	

	The solution should be able to give insights on hosts/users on the basis of Indicators of Compromise. Any license required for this should be included from day one.	
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
	The management platform support running on-demand and scheduled reports	
	The management platform must risk reports like advanced malware, attacks and network	
	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.	
Support	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement	
Hardware	**Temperature Operating:** 0 to 40°C	
	Temperature Nonoperating: - 40 to 65°C	
	Humidity: 5 to 95% noncondensing	
Power Supply	Should have redundant power supply for each appliance	

Architectural Requirements	**Compliance (Yes/No)**
The proposed solution must be based mandatorily on recursive DNS analysis.	
The solution must have a minimal impact with the existing DNS infrastructure	
The threat intelligence must be consumed from the OEM facilities that serve the recursive DNS requests.	
The solution must offer several deployment options: either via an internal virtual forwarder, or pointing the forwarder of the existing authoritative DNS to the recursive service, or pointing the DNS configured on the Internal Proxy to the recursive service, without any additional physical hardware.	
The recursive DNS security must be:	
Easily deployable, simply changing the forwarders to the OEM recursive DNS.	
Delivered directly from the OEM's global network.	
Easy to manage and operate	

The solution must be applicable simultaneously to corporate users connecting from wired and wireless networks, with the possibility to define different policies based on different public IPs, and or internal networks, or Active Directory attributes (in case an internal virtual forwarder is necessary).	
Security Requirements	
The solution must be able to detect and block advanced malware regardless of the specific ports or protocols used by the malware.	
The solution must be able to detect and block malware using protocols different from HTTP/HTTPS.	
The solution must be able to detect and block advanced malware used for both opportunistic attacks and targeted attacks targeted for this specific organisation.	
The solution must be able to protect at least from the following categories of malware: botnets, exploit kits, drive-by, phishing.	
The solution must be able to detect and block, suspicious DNS requests returning RFC1918 compliant IP addresses not allowed to be routed on the Internet, or directed to Dynamic DNS services.	
The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures.	
The solution must leverage predictive intelligence and not use static signatures or blacklists	
The predictive intelligence must be created via the DNS traffic analysis on a global scale, via a network of at least 20 distributed datacentres hosting the resolvers.	
The analysis algorithms must be enforce predictive detectors able to identify in real time, where attacks are staged and consequently predict and prevent the next move of attackers.	
In order to allow the malware detection on a global scale, the network utilised to build the threat intelligence must process at least **100 billion+** DNS requests/day coming from at least **60 million** daily users.	
The solution must have a proven efficacy being able to block at least 80 millions+ of daily DNS requests.	
The analysis algorithms must make use multi-layer predictive detectors. As a mere example, these include (but are not limited to):	
Analysis of DNS co-occurrences,	
Analysis of Domains based on Natural Language Processing algorithms.	
Detection of DGA via perplexity and entropy.	
Detection of DNS traffic peaks	
Soundwave analysis applied to DNS traffic	
BGP anomalies detection.	

The threat intelligence must be automatically updated in less than 15 minutes after the discovery of a new threat without any manual update operations.	
The solution must include a transparent intelligent proxy configurable inside each security policy and able to analyse both HTTP and HTTPS traffic.	
The transparent proxy must be enforced without any explicit mechanism such as a proxy PAC file or an adapter inside the network device.	
The solution must be able to enforce Web filtering policies, based on 90 +categories. It must be possible to enforce the Web filtering policy independently form the security policy.	
The web filtering and security policies must allow the creation of global exceptions for several domains, via custom whitelists or blacklists.	
For each domain detected as malicious, the solution must allow to visualise the IoCs and the features of this domain inside a dedicated investigation dashboard.	
The solution must have Ability to calculate risk score of apps compiled from 3 elements: Business, Usage, and Vendor Compliance.	
The solution must have Ability to showcase App Details When you click an app to open its detail view, you can check information including its risk score, type, category, users that have used it and detection date	
The solution must have Ability to show Workflow management via labeling of unreviewed and recently discovered apps to facilitate healthy cloud adoption.	
The solution must have Ability to block over 200 apps+ and automatically enable app settings and policy configuration.	
The solution must have Ability sbow DNS Requests by App Risk & assigns a risk score to apps, based on a number of factors. The DNS requests made by a high-risk app can be considered more problematic than the same number of requests made by an app with a lower risk score.	
The solution shall provide the capability for the administrator to classify public SaaS applications as Corporate Sanctioned official ones or personal instances and block them if need by	
Chromebook client Support	
The solution must have Chromebook client support to provides DNS-layer protection for Chromebook users whether they are connected to your networks or remotely, no matter which Chromebook device they use	
The solution must have Ability to Protect against phishing threats automatically with Umbrella's global network data and predictive intelligence to discover internet infrastructure used to host phishing sites.	
The solution must have Ability to Enhanced visibility to the user internet activity by logging user email to the Internet logs	
The solution must have Ability to Enforce policies to block in-appropriate content	
Management Requirements	

The management interface must be web-based. It must allow to create different user profiles with different level of permissions. As an example the roles must include:	
Administrator	
Reporting User	
Read-Only Users	
The management interface must provide a graphical policy editor to define security and web filtering policies.	
The policy editor must allow the creation of security policies based on identities such as networks, users, computers.	
Security Policies must allow the creation of distinct security and web filtering profiles.	
The policy editor must have a test function to verify the identities matching a security policy prior to its deployment in production.	
The policy editor must allow to define a blocking page for the blocked DNS connections.	
It must be possible to customise the blocking page for each policy entry. The customisation must include the ability to define a custom message, insert a custom logo, or an administrator email address.	
The policy editor must allow to define a different blocking page for each identity and category of events (for instance a blocking page for security-related events, a blocking page for web filtering blocks, etc.)	
The policy editor must allow to forward the blocked connection to an internal URLs.	
The policy editor must allow to create users, on a local database, with the ability to bypass the blocking page.	
The policy editor must allow to create special codes that allow to bypass the block pages for the users who have them.	
The events related to all the DNS queries analysed must appear in real time, with the ability to configure filters based on identity, destination, source IP, response type and date.	
The events related to the DNS queries associated to security events must appear in real time, with the ability to configure filters based on identity, destination, source IP and date.	
All the filters must be applicable defining a custom time (filter by date).	
All the filters must be applicable selecting web filtering categories and/on security categories.	
The dashboard must allow to reclassify a domain related to a security event, directly from the event record, via a link allowing to open a ticket towards the security OEM research team.	

In order to identify targeted attacks, the dashboard must be able to show the global DNS activity on each configured site, identifying in real time the targeted attacks comparing the local DNS traffic to a specific domain with the worldwide DNS traffic for the same domain.	
The dashboard must show an overview of all the traffic of the local organisation, with the ability to identify the prevented infections, the contained infections, and the blocks due to the web filtering policy.	
The management platform must have advanced reporting capabilities to identify cloud services or *Shadow IT* devices, in order to determine which services are used inside the organization by traditional or embedded devices and eventuallly detect anomalies in their usage.	
The management platform must allow to generate the following reports:	
Total requests	
Activity volume	
Top Domains	
Top Categories	
Top Identities.	
All the reports must be exported in csv format or scheduled to be sent via email.	
All the activities made by administrators must be logged inside an Admin Audit Log Report.	
The management interface must support 2 Factor Authentication mechanisms for the administrators, such as, for instance text messages or Google Authenticator.	
As an additional authentication mechanism for the administrators, the management interface must support the SAML integration with a SSO provider.	
Integration Requirements	
The connector must use the EDNS0 protocol (RFC6891).	
The solution must be able to extend the protection off the network through the installation of a lightweight roaming agent on the Windows and OSX devices.	
The agent must be also available as a profile for the VPN Client.	
The agent must be able to enforce a dedicated set of security and web filtering policies for the external users, or also transparently extend the internal corporate policies when the endpoint is outside the organization.	
The roaming agent must be deployable via GPO or an MSI package.	
The roaming agent must be lightweight, running in user mode, and transparent, meaning that it must not make use of Proxy PAC files or other explicit forwarding mechanisms.	
The roaming agent must be able to apply an additional level of enforcement based on the analysis of the connections trying to connect directly to an IP without generating and DNS queries (*IP Layer Enforcement*).	

It must be possible to selectively enable the IP Layer Enforcement inside each security policy.	
Resiliency and reliability requirements	
The network used to deliver the DNS security service must use *Anycast*.	
The network used to deliver the DNS security service must have experienced an *uptime* of at least 99.9% over the last 12 years.	
Support requirements	
It is required a support service including:	
§ Access to Online support via *Knowledge Base*, Forum, Documentation, Case Portal and notifications.	
§ 24X7X365 Phone Access for Priority 1 Cases.	
§ 12X5 Phone Access for Priority 2 and Priority 3 Cases.	
The support service must be delivered directly by the security OEM.	