भाकृअनुप - केन्द्रीय बारानी कृषि अनुसन्धान संस्थान

ICAR - Central Research Institute for Dryland Agriculture

संतोषनगर, सैदाबाद-पोस्ट हैदराबाद ५०००५९ **Santoshnagar, Saidabad P.O. Hyderabad 500 059**

040-24530161,24530163,24530224 Fax:040-24531802 www.crida.in Email : stores@crida.in

F. No: 9-1/(26)/2016/ST /NICRA Date: 15.10.2016

Sub: Quotation is invited for Next Generation Firewall– Reg.

Dear Sir (s),

Quotations are invited for following items cited below:

S. No	Name of the Items
1	Next Generation Firewall **(Specifications are enclosed herewith in Annexure)**

TERMS & CONDITIONS

1. The last date for submission of quotation is on or before **7-11-2016**. Rates offered shall be F.O.R. CRIDA, Hyderabad
2. Quotations should be sent by post only in a sealed cover addressed to the Director, Central Research Institute for Dry land Agriculture, Santoshnagar, Saidabad Post, Hyderabad – 500 059. The cover containing quotation should invariably be super scribed. The quotations in person by hand will not be accepted.
   a. **Enquiry F. No: 9-1/(26)/2016/ST/NICRA**
   b. **Due on 7-11-2016**
   c. **For Next Generation Firewall**
3. The quotation should remain open for acceptance for a period of 90 days from the date (due date)
4. An earnest money of **Rs. 10,000/- (Rupees Ten thousand only)** should be deposited in the form of Demand Draft / Banker's Cheque in favour of **'ICAR Unit - CRIDA'** payable at Hyderabad. The quotation will not be considered if earnest money is not deposited with the tenders.
5. The earnest money would be refunded to all the unsuccessful bidders . For Successful bidders the earnest money would be refunded only after deposition the Security deposit/Performance Guarantee.
6. **An amount of 10% of total order value as Security Deposit (Performance Guarantee) in the form of DD/ PO/Bank Guarantee/FDR** is to be deposited by the successful Bidder only after receiving a communication from the Institute. In the event of non-deposition of the same within 15 days of the communication, the earnest money will be forfeited. In the event of any default of performance or conditions of supply, the security deposit will be forfeited.
7. No advance payment/delivery against payment is permissible. However, the payment shall be arranged in 10 days from the date of submission of pre-receipted bill in triplicate along with stores.
8. The rates quoted should be net payable for each item for delivery at the Institute at the address given above (inclusive of all taxes, packing, forwarding, transport, insurance and excluding rebate/discount etc.)
9. This Institute is not in a position to supply any ' D ' or 'C' forms.
10. While quoting the rates please mention the following:

- Approximate time for supply of stores from the date of placing order.
- Guarantee/Warranty/Expiry period
- In case you have got any rate contract with the DGS&D, the same may be indicated
- Any other condition

Quotation which do not conform to the above terms and conditions will not be considered. The Director, Central Research Institute for Dryland Agriculture, reserves the right to accept or reject any or all quotations without assigning any reasons thereof.

Yours Sincerely

(Er C V K N Rao)
Stores and Purchase Officer

Technical Specifications for Next Generation Firewall

Technical Specifications for Next Generation Firewall
Firewall must be standard IU rack mountable
It must provide 1Gbps of threat mitigation throughput, combining application level firewall, IPS, Antivirus and Antispyware.
It must provide high performance with low latency for all application level inspection in real-time
It must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, QOS
The Firewall must be administered locally with user friendly GUI
The Firewall must have modern malware protection that identify unknown malicious files and execute them in a controlled environment to expose malicious behaviour even if the malware has never been seen before
The firewall should have at least 8 ports of 10/100/1000 Ethernet Ports and 2 x 1G-SFP ports
Minimum 8 GB memory and 120GB SSD drive
The firewall throughput of minimum 2 Gbps.
It must give 1 Gbps of firewall + IPS combined throughput
It shall handle Minimum 50,000 new sessions per second
It shall handle Minimum 200,000 concurrent sessions
It handling Minimum of 2000 policies
Operation Mode
The proposed solution must be able to support Network attack detection, DoS, DDoS,TCP Reassembly , Brute Force, Syn Cookie, IP Spoofing, Malformed Packet etc.
It should operate on Bridge mode/Traparent/Tap mode interface configuration
The firewall must support Transparent, Layer 2 , Layer 3 mode providing flexible deployment
The firewall should support simultaneous deployment with interfaces servicing Layer 3, Layer 2 Transparent
The firewall shall support 802.1Q VLAN tagging
The firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection under various deployment modes
The firewall shall support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth
The firewall shall support logical Ethernet sub-interfaces tagged and untagged.
The firewall must support the following routing protocols static, RIPv2, OSPF, BGP4
The firewall must have IPv6 Static Routing Support even for virtual routers
The firewall must have Virtual Router capability that supports all L3 capability
The firewall must support Policy Based forwarding based on Zone, Applications , Source / Destination Address, User or User Group
The firewall shall support DNS proxy
The OEM should ensure that the solution should be operational for 5 years, with all core feature / functionalities enabled on the platform.
Firewall must have IPv6 networking feature and ready from day one.
The Firewall must support DHCPv4 and DHCPv6 relay
Policy Based Controls
The proposed solution shall control parameters by Security Zone, Users, IP, Application, Host Information Profile, URL Category ,Schedule, QoS etc.
It shall be application based and protocol based

For application and/or application category
For application function (posting, file transfer, desktop sharing, instant messaging, etc.)
For user, group or IP address
Geography based Blocking
Decryption and Inspection of SSL traffic
-Block files by type: bat, cab, dll, exe, pif, reg and etc.
-Data filtering: Social Security Numbers, Credit Card Numbers, Custom Data Patterns, and etc.
-QoS Policy-based traffic shaping (priority, guaranteed, maximum)
-Policy support for scheduled time of day enablement
Application Security Policy
The firewall shall support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic without any additional licensing policy
The firewall shall identify application function and have decoding technology
The firewall shall handle unknown/unidentified applications e.g. alert, block or allow
The firewall shall create custom application signatures and categories
The firewall must allow updating the application database automatically or manually via the control or traffic plane
The firewall shall delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.)
The firewall shall delineate specific instances of instant messaging (AIM, YIM, Facebook Chat, etc.)
The firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability
The firewall shall delineate specific instances of Proxies (ultrasurf, ghostsurf, freegate, etc.)
The proposed solution shall support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)
Threat Prevention
The firewall must protect from Vulnerabilities , Virus, Spyware, Bot and malware etc.
The firewall shall block known network and application-layer vulnerability exploits
The firewall shall block buffer overflow, DoS/DDoS , etc. type of attacks
The firewall shall support attack recognition for IPv6 traffic the same way it does for IPv4
The firewall shall support Built-in Signature and Anomaly based Vulnerability Protection Engine
The firewall shall support the ability to create custom user-defined signatures
The firewall shall support granular tuning with option to configure overrides for individual signatures
The firewall shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)
The firewall must update Vulnerability / Virus / Spyware protection time to time without rebooting.
The firewall shall support several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc.
The firewall shall support response adjustment on a per signature basis.
The firewall shall support notifications via alerts, email notifications, SNMP traps and packet logs
URL Filtering
The firewall shall support URL-Filtering
The firewall shall have the database located locally on the device
The firewall shall support custom URL-categorization
The firewall shall support customizable block pages
The firewall shall support logs populated with end user activity reports for site monitoring within the local solution
The firewall shall support Drive-by-download control

The firewall shall support URL Filtering policies by AD user, group, machines and IP address/range
Data Filtering
The firewall shall support file identification based on signature and not file extensions
The firewall shall support identification and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via identified applications (i.e. P2P, IM, SMB, etc.)
The firewall shall support compressed information stored in zipped format and be able to unpack and filter per policy
The firewall shall be capable of identifying and preventing the transfer of files containing sensitive information (i.e. credit card numbers) via regular expression
User Identification and Authentication
The firewall must have authentication services for user-identification using any of the following technologies AD, LDAP, directory, Radius, Kerberos, Client Certificate without any additional licensing policy
The firewall should support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP
The firewall shall support user-identification in policy without installing an agent on individual endpoints
The firewall shall support user-identification from Citrix, google play, itunes etc. and terminal services environments in policy and logs
The firewall shall populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time
Quality of Service (QoS)
The firewall should create QoS policy on a per rule basis specifically by Applications e.g. web based videoconferencing application and Static or Dynamic Application Groups , such as P2P , IM groups
The firewall shall define QoS traffic classes with Guaranteed and Maximum bandwidth along with priority queuing , differ markings on packets
The firewall should support real-time prioritization of voice based protocols like H.323, SIP, SCCP, MGCP and applications like Skype, Videoconference, webex, etc
Secure Sockets Layer (SSL) Decryption
The Firewall shall identify, decrypt and evaluate SSL traffic in an outbound and inbound connections (forward-proxy)
The firewall should support decryption and inspection of SSL traffic in an outbound connection, inbound connection across any port"
The firewall shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic
Virtual Private Network (VPN)
The firewall shall support IPSec, SSL VPN and should be available
IPSec VPN should be integrated with the firewall and support full encryption standards
TCPDump / PCAP
The firewall shall support packet captures based on Source Address, Destination Address, Applications, Unknown Applications, Port, Threats, Data Filters and / or any combination as specified
The firewall shall support PCAP downloads of specific traffic sessions from the GUI from the logging screen
Modern Malware Prevention
The firewall shall support sandbox behavior based inspection and protection of unknown viruses and malware
The firewall shall support automated signature generation for discovered malware, coupled with auto-update on configured firewalls, ensuring that up to date protection is available against advanced attacks
The firewall shall support inline control of malware infection and command/control traffic

The firewall must have the flexibility of using a cloud based service or an on-premise appliance for malware analysis. A cloud based service would be preferred initially, but it should be possible to move from the cloud based service to an on-prem solution if needed.
The firewall must support Windows, Linux, MAC OS X and Android malware analysis
The firewall must provide integration with an automated intelligence tool provided by the OEM, providing visibility into attacks that are seen world-wide, with tags to highlight attacks of similar nature.
Intrusion Prevention System (IPS)
IPS must be an integrated system of Firewall
The Firewall must have signature based, behavioral based and protocol anomaly based Intrusion prevention system.
The Firewall must support creation of custom IPS signature
Integrated IPS should support hybrid attack detection/prevention with multiple attack protections methods, like Protocol Anomaly, Signature-Based, Day-Zero Protection, etc.
The IPS should be constantly updated with new defenses against emerging threats
Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related
Proposed Vendor Should have passed NSS Labs IPS test
Firewall logging and reporting system
The firewall should have built in storage capacity of at least 100GB for storing logs.
The firewall should have Reporting solution. The reports should be accessible through Http/Https based.
The administration software must provide a means of viewing, filtering and managing the log data
The firewall must have support for sending log information to an external log server via an encrypted connection
Firewall log analyser software must be installed and configured to get required reports
Installation and Configuration
Firewall and its applications must be installed completely at CRIDA and configured as per the requirements
Warranty and Service Support
Minimum 3 years comprehensive onsite on hardware, software and technical support