

No. M.V-12/2012-13-DA.IV.IT 841
भारत सरकार/Government of India
गृह मंत्रालय/Ministry of Home Affairs
पुलिस आधुनिकीकरण प्रभाग /Police Modernization Division
संभरण-I डेस्क /Prov.I Desk

26, Man Singh Road, Jaisalmer House,
New Delhi, dated the 21st April, 2015

To,

The DsG: AR, BSF, CISF, CRPF, ITBP, SSB, NSG & BPR&D.

Subject: QRs and Trial Directives of Firewall/Multi Functional Security Appliance.

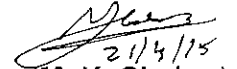
Sir,

The undersigned is directed to refer to the subject mentioned above and to say that the QRs and Trial Directives in respect of Firewall/Multi Functional Security Appliance as per Annex-I and Annex-II, respectively have been approved by the competent authority in MHA.

2. Henceforth, all the CAPFs should trial evaluate and procure the above item, required by them, strictly as per the laid down QRs.

3. Concerned CAPF will be accountable for correctness of the QRs and Trial Directives of Firewall/Multi Functional Security Appliance.

Yours faithfully,



21/4/15
(M. K. Chahar)

Under Secretary to the Govt. of India

Encl: As above.

Copy forwarded for necessary action to:

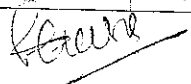
✓ SO (IT), MHA - with the request to host the QRs and Trial Directives of Firewall/Multi Functional Security Appliance on official website of MHA (under the page of Organizational Set up, Police Modernization Division-Communication Equipments). Soft copy is being sent through email also.

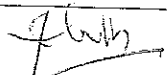

(R. K. Soni)
Section officer (Prov-I)

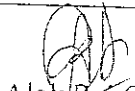
Copy to: DDG (Procurement), MHA


Item No.	Item / Work Description with Configuration																
1.	MFSA																
	Must support the following parameters with CPU utilization < 50%																
	<table border="1"> <thead> <tr> <th rowspan="2">No. of Concurrent Users</th> <th colspan="3">Throughput (in Mbps)</th> <th rowspan="2">Network Ports (10 / 100 / 1000 Mbps)</th> <th rowspan="2">Concurrent connections per second</th> <th rowspan="2">New connections per second</th> </tr> <tr> <th>Only Firewall</th> <th>Firewall + IPS</th> <th>Firewall + IPS + Anti-virus</th> </tr> </thead> <tbody> <tr> <td>250</td> <td>1000</td> <td>500</td> <td>300</td> <td>Minimum 6 Nos.</td> <td>2 Lakhs or more</td> <td>10 K or more</td> </tr> </tbody> </table>	No. of Concurrent Users	Throughput (in Mbps)			Network Ports (10 / 100 / 1000 Mbps)	Concurrent connections per second	New connections per second	Only Firewall	Firewall + IPS	Firewall + IPS + Anti-virus	250	1000	500	300	Minimum 6 Nos.	2 Lakhs or more
No. of Concurrent Users	Throughput (in Mbps)			Network Ports (10 / 100 / 1000 Mbps)	Concurrent connections per second				New connections per second								
	Only Firewall	Firewall + IPS	Firewall + IPS + Anti-virus														
250	1000	500	300	Minimum 6 Nos.	2 Lakhs or more	10 K or more											
2.	MFSA Model-1 HA: MFSA device for High-Availability of MFSA Model-1																
3.	MFSA Log Analysis solution																

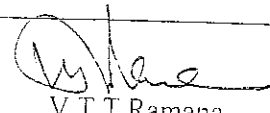
S. No.	MFSA SPECIFICATION
1.	Details:
1.1.	Throughput supported by the device (in Mbps)
	1.1.1 Firewall Throughput
	1.1.2 Firewall + IPS (All signatures enabled) Throughput
	1.1.3 Firewall + IPS (All signatures enabled) + Antivirus Throughput (flow-based / proxy-based)
1.2.	Concurrent Sessions supported with all modules enabled
	New connections per second
1.3.	Rack space (1U/ 2U, etc.)
1.4.	Operating Voltage- 110-240V AC
1.5.	Temperature – 5 to 40°C
1.6.	AC Frequency – 50/60 Hz
	MFSA SPECIFICATION (Mandatory)
2.	GENERAL
2.1.	The MFSA device must have the following Integrated functions / modules:


S.M. Hasnain
(DIG-IT, CRPF)

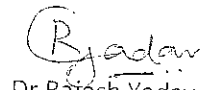

Jagjit Singh
(TD, NIC)


Alok Rai Choudhary
(TD, NIC)

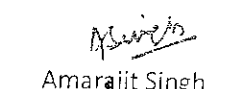

D.A.K. Khan
(STD, NIC)



V.T.T. Ramana
(TD, NIC)


Dhruva Jyoti Sharma
(TD, NIC)


Dr Rajesh Yadav
(TCG, DRDO)


Kapil
(SSA, BPR&D)

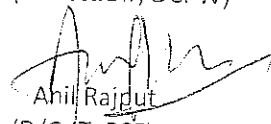

Amarajit Singh
(E.Asstt. Dir, DCPW)

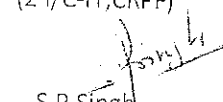

D.K. Singh
(2 I/C-IT, CRPF)

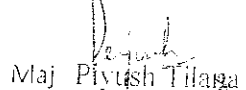

Jayasankar M.N
(A/C-IT, CRPF)



Kulwinder Singh
(Insp/Tech-CRPF)

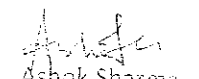

Anil Kamboj
(SI/Tech-CRPF)

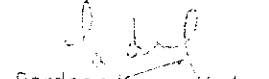

Anil Rajput
(D/C-IT, BSF)

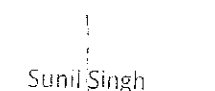

S.P. Singh
(Insp/Comn, BSF)


Maj Piyush Tilaga
(NSG)

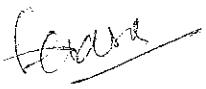
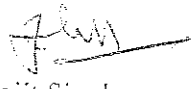




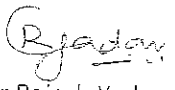
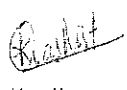
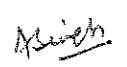

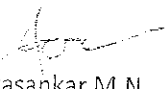
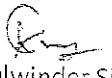

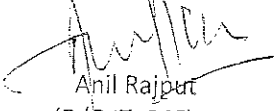
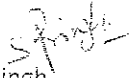
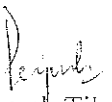

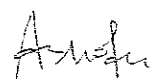
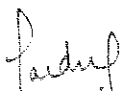
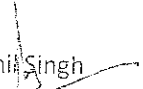

R.K. Kumbhare
(A/C-Comn, SSB)


Ashok Sharma
(Insp/Comn, SSB)


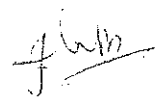

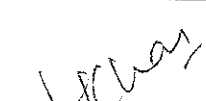
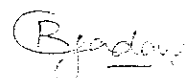


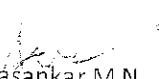
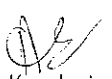
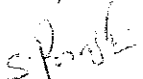



Pardeep Kumar Yadav
(A/C-ITBP)


Sunil Singh
(SI/RT-ITBP)

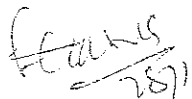
	2.1.1 Firewall
	2.1.2 Intrusion Prevention System (IPS)
	2.1.3 Anti-virus
	2.1.4 URL Filtering
	2.1.5 Traffic Snapping
	2.1.6 Virtual Private Network
	2.1.7 Application Control
2.2.	High-Availability of MFSA device
	2.2.1 All MFSA functions mentioned at point no. 2.1 must work in High-Availability mode.
2.3.	The MFSA license must not have restriction on number of users or IP addresses for all MFSA functions / modules mentioned in point no. 2.1 .
2.4.	The device must be deployable in routing mode.
2.5.	The device must support the following routing protocols.
	2.5.1 BGP
	2.5.2 OSPF
2.6.	The device must be deployable in bridge (transparent) mode.
	2.6.1 All MFSA modules must work in bridge mode except point no. 2.1.6.
	2.6.2. BGP protocol packets must pass through transparently in bridge mode.
	2.6.3. Must support multicast packets in bridge mode.
2.7.	The device must support multiple network subnets on a physical network interface.
2.8.	Video & Voice support:
	2.8.1 Must be session-aware to inspect various Video & voice protocols, such as, H.323 and Session Initiation Protocol (SIP) protocols.
2.9.	The device must support Dual-Stack IPv4 and IPv6 for all MFSA modules.
2.10.	Logging and Monitoring:
	2.10.1. It must be able to send logs to external syslog server and MFSA Log analysis Solution.

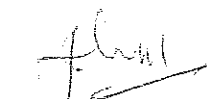
 S.M. Hasnain (DIG-IT, CRPF)	 Jagjit Singh (TD, NIC)	 Alok Rai-Choudhary (TD, NIC)	 D.H. Khan (STD, NIC)	 V.T.T Ramana (TD, NIC)
 Dhruba Jyoti Sharma (TD, NIC)	 Dr Rajesh Yadav (TCG, DRDO)	 Kapil (SSA, BPR&D)	 Amarajit Singh (E.Asstt. Dir, DCPW)	 D.K. Singh (2 I/C-IT, CRPF)
 Jayasankar M.N (A/C-IT, CRPF)	 Kulwinder Singh (Insp/Tech-CRPF)	 Anil Kamboj (SI/Tech-CRPF)	 Anil Rajput (D/C-IT, BSF)	 S.P. Singh (Insp/Comn, BSF)
 Maj Piyush Tilana (NSG)	 R.K. Kumbhare (A/C-Comn, SSB)	 Ashok Sharma (Insp/Comn, SSB)	 Pardeep Kumar Yadav (A/C-ITBP)	 Sunil Singh (SI/RT-ITBP)

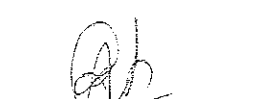
2.11.	Device Management:					
	2.11.1 The device must be manageable from Centralised Management Solution.					
	2.11.2 The device must support role based administration.					
	2.11.3 The device must support management over secure channel.					
	2.11.4. The device must restrict management from specified IP addresses / networks.					
	2.11.5 The device must support AAA authentication					
2.12.	Certifications:					
	2.12.1. The MFSA modules must have one of the given certifications. Tick the certificate for each of the MFSA functions / modules:	EAL4	ISO 15408	Check mark	ICSA Labs	NSS Labs
	2.12.1.1. Firewall & VPN modules					
	2.12.1.2. Antivirus module					
	2.12.1.3. IPS module					
2.13.	Warranty & Software subscription:					
	2.13.1. Five years on-site comprehensive warranty support					
	2.13.2 Five years software subscription support					
3.	FIREWALL					
3.1.	Must be a Stateful packet inspection firewall.					
3.2.	Firewall module must support security policies (firewall rules) based on:					
	3.2.1 IP address					
	3.2.2 Network subnet					
	3.2.3. Protocol (TCP, UDP, ICMP, etc.)					
	3.2.4 Services					
	3.2.5 Time					
	3.2.6 User-group					
3.3.	Must have provision to create local users on the device to support user based security policies					

 S.M. Hasnain (DIG-IT, CRPF)	 Jagjit Singh (TD, NIC)	 Alok Rai Choudhary (TD, NIC)	 D.H.Khan (STD, NIC)	 V.T.T Ramana (TD, NIC)
 Dhruva Jyoti Sharma (TD, NIC)	 Dr Rajesh Yadav (TCG, DRDO)	 Kapil (SSA, BPR&D)	 Amarajit Singh (E. Asstt. Dir, DCPW)	 D.K. Singh (2 I/C-IT, CRPF)
 Jayasankar M.N (A/C-IT, CRPF)	 Kulwinder Singh (Insp/Tech-CRPF)	 Anil Kamboj (SI/Tech-CRPF)	 Anil Rajput (D/C-IT, BSF)	 S.P. Singh (Insp/Comn, BSF)
 Maj Piyush Tilaga (NSG)	 R.K. Kumbhare (A/C-Comn, SSB)	 Ashok Sharma (Insp/Comn, SSB)	 Pardeep Kumar Yadav (A/C-ITBP)	 Sunil Singh (SI/RT-ITBP)

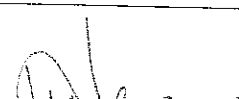
3.4.	Must integrate with the following third-party authentication services to support user based security policies:
	3.4.1 LDAP
	3.4.2 Windows Active Directory
3.5.	Network Address Translation (NAT): Must support the following:
	3.5.1 Dynamic NAT
	3.5.2 Static NAT
	3.5.3 PAT
	3.5.4 No-NAT (traffic should pass without IP address translation)
	3.5.5 Policy based source and destination NAT
4.	INTRUSION PREVENTION SYSTEM (IPS)
4.1.	The IPS must be able to detect and respond (block, notify) to any malicious activity.
4.2.	Must be possible to configure traffic-direction based IPS polices.
4.3.	Must support creation of user-defined signatures.
4.4.	IPS must support exemption of traffic inspection for:
	4.4.1 Specific IP addresses
	4.4.2 Networks (source and destination separately)
4.5.	Must be possible to block / allow files based on:
	4.5.1 File names
	4.5.2 File extensions
	4.5.3 File types
4.6.	Day Zero protection.
4.7.	Identity & Block DoS&DDoS. Sync flagged & encrypted attacks.
4.8.	Custom Signature Support.
4.9.	Should defend & monitor against worms, virus, Trojan
4.10.	Role based access to various IPS Policies.


S.M. Hasnain
(DIG-IT, CRPF)



Jagjit Singh
(TD, NIC)


Alok Rai Choudhary
(TD, NIC)

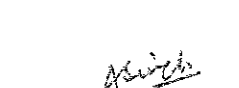

D.H. Khan
(STD, NIC)

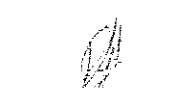

V.T.T Ramana
(TD, NIC)



Dhruva Jyoti Sharma
(TD, NIC)


Dr Rajesh Yadav
(TCG, DRDO)


Kapil
(SSA, BPR&D)



Amarajit Singh
(E.Asstt.Dir, DCPW)



D.K. Singh
(2 I/C-IT, CRPF)


Jayasankar M.N
(A/C-IT, CRPF)



Kulwinder Singh
(Insp/Tech-CRPF)

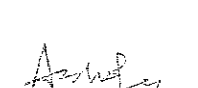

Anil Kamboj
(SI/Tech-CRPF)

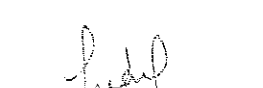

Anil Rajput
(D/C-IT, BSF)

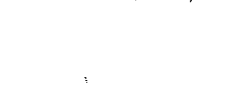

S.P. Singh
(Insp/Comn, BSF)


Maj Piyush Tilaña
(NSG)


R.K. Kumbhare
(A/C-Comn, SSB)


Ashok Sharma
(Insp/Comn, SSB)

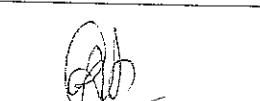

Pardeep Kumar Yadav
(A/C-ITBP)

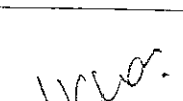

Sunil Singh
(SI/RT-ITBP)

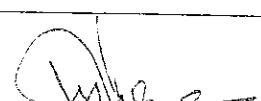
5.	ANTIVIRUS
5.1.	Gateway Antivirus must provide real-time protection of viruses, worms, Trojans and other malicious code (like spyware, adware, etc.) at the gateway for SMTP, POP3, IMAP, HTTP, HTTPS, FTP & IM traffic in both directions.
6.	URL FILTERING
6.1.	URL filtering must work for HTTP and HTTPS traffic
6.2.	The following security related URL categories must be supported in addition to the other categories
	6.2.1. BOTNETs
	6.2.2. Malicious sites
	6.2.3. Phishing sites
	6.2.4. SPAM sites
	6.2.5. HACKING
	6.2.6. Proxy avoidance / remote proxy
	6.2.7. P2P file sharing
6.3.	URL filtering must be possible for specified:
	6.3.1 IP address
	6.3.2 Network subnet
	6.3.3 User-group
6.4.	Must be possible to block / allow
	6.4.1 URLs based on categories.
	6.4.2 Unrated sites.
	6.4.3 User-defined URLs.
6.5.	Must have provision to block / allow:
	6.5.1 Web based chat traffic
	6.5.2 Peer to peer traffic
	6.5.3 Voice traffic
	6.5.4 Video traffic
6.6.	The solution must be able to block sites containing:
	6.6.1. Spywares



S.M. Hasnain
(DIG-IT, CRPF)

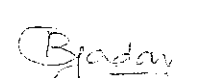

Jagjit Singh
(TD, NIC)


Alok Rai Choudhary
(TD, NIC)


D.H. Khan
(STD, NIC)


V.T.T Ramana
(TD, NIC)

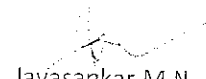

Dhruva Jyoti Sharma
(TD, NIC)


Dr Rajesh Yadav
(TCG, DRDO)


Kapil
(SSA, BPR&D)


Amarajit Singh
(E.Asstt.Dir, DCPW)

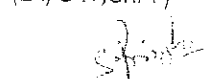

D.K. Singh
(2 I/C-IT, CRPF)


Jayasankar M.N
(A/C-IT, CRPF)



Kulwinder Singh
(Insp/Tech-CRPF)



Anil Kamboj
(SI/Tech-CRPF)

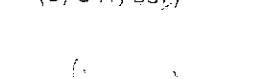

Anil Rajput
(D/C-IT, BSF)

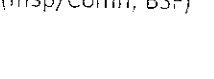

S.P. Singh
(Insp/Comn, BSF)


Maj Piyush Tilana
(NSG)

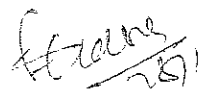

R.K. Kumhare
(A/C-Comn, SSB)

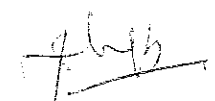

Ashok Sharma
(Insp/Comn, SSB)



Pardeep Kumar Yadav
(A/C-ITBP)


Sunil Singh
(SI/RT-ITBP)


	6.5.2	Adwares
	6.5.3	Malwares
6.7.	Must have configurable options to allow/deny access to web sites when the URL rating service is unavailable	
7.	TRAFFIC SHAPING	
7.1.	Must be possible to enable Traffic Shaping(rate limiting) for specified:	
	7.1.1	IP address
	7.1.2	Network subnet
	7.1.3	Services
7.2.	Must be possible to configure Guaranteed bandwidth for specified:	
	7.2.1	IP address
	7.2.2	Network subnet
	7.2.3	Services
7.3.	Must be possible to configure Maximum bandwidth for specified:	
	7.3.1	IP address
	7.3.2	Network subnet
	7.3.3	Services
8.	VIRTUAL PRIVATE NETWORK (VPN)	
8.1.	The device must support IPSEC VPN protocol.	
8.2.	The device must support site to site VPN	
8.3.	The device must support remote-client VPN. Must include client licenses, if any, for the number of users mentioned in the technical specifications of the Item.	
8.4.	The device must scan all VPN traffic for malicious content.	
9.	APPLICATION CONTROL	
9.1.	Must discover applications automatically and enable application policy controls independent of port and protocol.	
9.2.	The device must be able to allow / deny applications based on:	
	9.2.1	Specified users


S.M. Hasnain
(DIG-IT, CRPF)



Jagjit Singh
(TD, NIC)



Alok Rai Choudhary
(TD, NIC)


D.H. Khan
(STD, NIC)



V.T.T Ramana
(TD, NIC)



Dhruva Jyoti Sharma
(TD, NIC)


Dr Rajesh Yadav
(TCG, DRDO)


Kapil
(SSA, BPR&D)


Amarajit Singh
(E.Asstt. Dir, DCPW)

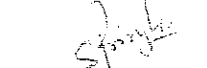

D.K. Singh
(2 I/C-IT, CRPF)

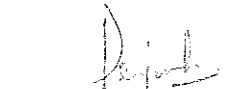

Jayasankar M.N
(A/C-IT, CRPF)


Kulwinder Singh
(Insp/Tech-CRPF)

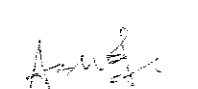

Anil Kamboj
(SI/Tech-CRPF)

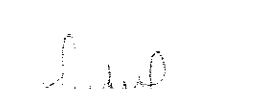

Anil Rajput
(D/C-IT, BSF)



S.P. Singh
(Insp/Comn, BSF)


Maj Piyush Tilaga
(NSG)

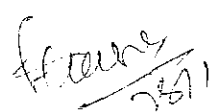

R.K. Kumbhare
(A/C-Comn, SSB)

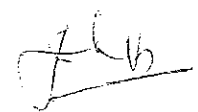

Ashok Sharma
(Insp/Comn, SSB)



Pardeep Kumar Yadav
(A/C-ITBP)


Sunil Singh
(SI/RT-ITBP)

9.2.2	Specified user groups
9.2.3	Specified user groups with exceptions
9.2.4	Specified source IPs
9.2.5	Specified source Networks
9.3.	The device must identify and control Web 2.0 applications
S. No.	SPECIFICATION FOR MFSA LOG ANALYSIS SOLUTION
1.	Specify:
	1.1. Item No.
	1.2. OEM
	1.3. Model
	1.4. Rack space (1U, 2U, etc.)
	1.5. Power requirement (in Watts)
2.	Must be accessible through GUI.
3.	Must be accessible over secure channel.
4.	A single Log Analysis solution must support / be
	4.1. 100 or more MFSA devices
	4.2. Storage space of 2 TB or more
	4.3. RAID 5 redundancy
	4.4. Rack mountable
	4.5. 5000 Events Per Second (EPS)
5.	Must have provision to view and analyze real-time alerts from all MFSA devices.
6.	Drilldown facility must be available for alert monitoring.
7.	Must generate the following reports:
	7.1. Attack reports
	7.2. Bandwidth usage reports
	7.3. Source IP/ destination IP reports


S.M. Hasnain
(DIG-IT, CRPF)

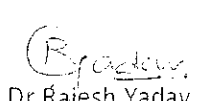

Jagjit Singh
(TD. NIC)


Alok Rai Choudhary
(TD. NIC)

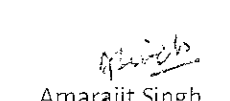

D.H. Khan
(STD, NIC)



V.T.T Ramana
(TD. NIC)

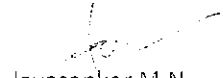

Dhruva Jyoti Sharma
(TD, NIC)


Dr Rajesh Yadav
(TCG, DRDO)


Kapil
(SSA, BPR&D)



Amarajit Singh
(E. Asstt. Dir, DCPW)

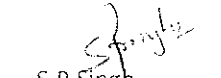

D.K. Singh
(2 I/C-IT, CRPF)



Jayasankar M.N
(A/C-IT, CRPF)

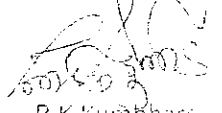

Kulwinder Singh
(Insp/Tech-CRPF)

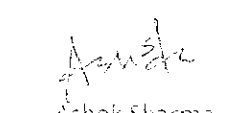

Anil Ramboj
(SI/Tech-CRPF)

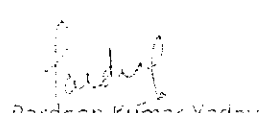

Anil Rajput
(D/C-IT, BSF)



S.P. Singh
(Insp/Conn, BSF)


Ma: Piyush Tilagta
(NSG)


R.K. Kumbhare
(A/C-Conn, SSB)


Ashok Sharma
(Insp/Conn, SSB)


Pardeep Kumar Yadav
(A/C-ITBP)


Sunil Singh
(SI/RT-ITBP)

	7.4. Source network / destination network reports
	7.5. User based reports
	7.6. Service based reports
	7.7. URL based reports
	7.8. Access or Denied reports
	7.9. User-defined reports
8.	The solution must have provision to export log of a particular device as a text file for the specified period without any restriction on number of log entries or the size of the log file
9.	The solution must have configurable option to schedule the report generation.
10.	Must support sending the scheduled reports to the designated email addresses.
11.	Role based access for the log analyzer:
	11.1. Must be possible to allow a given user to analyze the logs of one or more MFSA devices.
	11.2. Must support multiple roles like administrator, operator etc for the log analyzer.
	11.3. Remote access to the log analyzer must be possible from specific IP addresses / subnets only.
12.	Warranty & Software subscription:
	12.1 Five years on-site comprehensive warranty support
	12.2. Five years software subscription support.
	12.3. Management should support CLI/GUI

S.M. Hasnain
(DIG-IT, CRPF)

Jagjit Singh
(TD, NIC)

Alok Rai Choudhary
(TD, NIC)

D.H. Khan
(STD, NIC)

V.T.T Ramana
(TD, NIC)

Dhruba Jyoti Sharma
(TD, NIC)

Dr Rajesh Yadav
(TCG, DRDO)

Kapil
(SSA, BPR&D)

Amarajit Singh
(E.Asstt.Dir, DCPW)

D.K. Singh
(2 I/C-IT, CRPF)

Jayasankar M.N
(A/C-IT, CRPF)

Kulwinder Singh
(Insp/Tech-CRPF)

Anil Kamboj
(SI/Tech-CRPF)

Anil Rajput
(D/C-IT, BSF)

S.P. Singh
(Insp/Comn, BSF)

Maj Piyush Tilaga
(NSG)

R.K. Kumbhare
(A/C-Comn, SSB)

Ashok Sharma
(Insp/Comn, SSB)

Pardeep Kumar Yadav
(A/C-ITBP)

Sunil Singh
(SI/RT-ITBP)

Shailendra Kumar
(IGP-Comn&Works)

APPROVED / NOT APPROVED.

Pavash Mishra
DG CRPF

19861

TRIAL DIRECTIVE OF MULTI-FUNCTIONAL SECURITY APPLIANCE (MFWA/FIREWALL) :

Item No.	Item / Work Description with Configuration	Trial directive																	
MFWA	Must support the following parameters with CPU utilization < 50%																		
1.	<table border="1"> <thead> <tr> <th colspan="3">Throughput (in Mbps)</th> <th rowspan="2">Network Ports (10 / 100 / 1000 Mbps)</th> <th rowspan="2">Concurrent connections per second</th> <th rowspan="2">New connections per second</th> </tr> <tr> <th>No. of Con-current Users</th> <th>Only Firewall all</th> <th>Firewall + IPS</th> <th>Firewall + IPS + Anti-virus</th> </tr> </thead> <tbody> <tr> <td>250</td> <td>1000</td> <td>500</td> <td>300</td> <td>Minimum 6 Nos.</td> <td>2 Lakhs or more</td> <td>10 K or more</td> </tr> </tbody> </table>	Throughput (in Mbps)			Network Ports (10 / 100 / 1000 Mbps)	Concurrent connections per second	New connections per second	No. of Con-current Users	Only Firewall all	Firewall + IPS	Firewall + IPS + Anti-virus	250	1000	500	300	Minimum 6 Nos.	2 Lakhs or more	10 K or more	Verify from product catalogue and match with supplied product & by physical verification
Throughput (in Mbps)			Network Ports (10 / 100 / 1000 Mbps)	Concurrent connections per second				New connections per second											
No. of Con-current Users	Only Firewall all	Firewall + IPS			Firewall + IPS + Anti-virus														
250	1000	500	300	Minimum 6 Nos.	2 Lakhs or more	10 K or more													
2.	<p>MFWA Model-1 HA: MFWA device for High-Availability of MFWA Model-1</p>																		
3.	MFWA Log Analysis solution																		

Handwritten signatures and names:

S. M. Hasnain (DICT, GRC/IT), Jagjit Singh (DICT, SEC)

Alok Kumar Bhandary (DICT, SEC), D. K. Singh (DICT, SEC)

V. V. Ramana (DICT, SEC), Dhruva Jyoti (DICT, SEC)

Sharna (DICT, SEC), Dr. Rajesh Yadav (DICT, SEC), Kishor (DICT, SEC)

Amrajit Singh (DICT, SEC), D.K. Singh (DICT, SEC)

Jayasankar M.N. (A/C-IT, CRP), Kulvinder Singh (DICT, SEC)

Anil Kumbhoj (SIV/tech-CRP), Anil Kumbhoj (DICT, SEC)



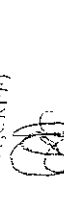
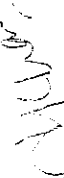

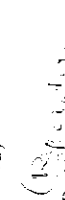
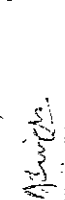


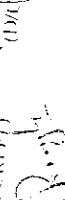
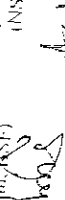

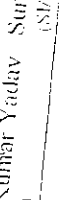


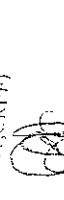
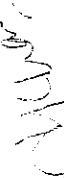

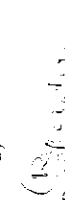
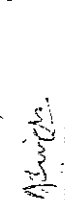


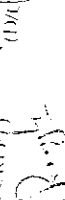
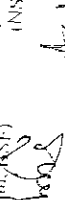

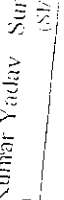
S.P. Singh (DICT, SEC), Manj. Divyash Hegde (DICT, SEC)

R.K. Kumbhare (A/C-Comm, SSR), Ashok Sharma (DICT, SEC)

Pandit Kumar Yadav (A/C-IT), Sumit Singh (DICT, SEC)

(155)

S. No.	MPSA SPECIFICATION Details:	Remarks	Signature	Name & Designation
1.1.	Throughput supported by the device (in Mbps)			
1.1.1.	Firewall Throughput	Verify from product catalogue and match with supplied product		
1.1.2.	Firewall + IPS (All signatures enabled)	Verify from product catalogue and match with supplied product		
1.1.3.	Firewall + IPS (All signatures enabled) + Antivirus Throughput (flow-based / proxy-based)	View in Technical guide and verify features using Console / Web console		
1.2.	Concurrent Sessions supported with all modules enabled	View in Technical guide and verify features		
1.2.1.	New connections per second	View in Technical guide and verify features		
1.3.	Rack space (1U/ 2U, etc.)	View in Technical guide and verify features		
1.4.	Operating Voltage- 110-240V AC	View in Technical guide and verify features		
1.5.	Temperature - 5 to 40°C	View in Technical guide and verify features		
1.6.	AC Frequency - 50/60 Hz	View in Technical guide and verify features		
	MPSA SPECIFICATION (Mandatory)			
	GENERAL			
2.1.	The MPSA device must have the following Integrated functions / modules:			
2.1.1.	Firewall	View in Technical guide and verify features using Console / Web console		

 S.M.H. Hasnain (Dir-IT, CRPF)
 Jagjit Singh (TD, NIC)
 Alok Nath Choudhary (TD, NIC)
 D.K. Khan (TD, NIC)
 V.V. Ramana (TD, NIC)
 Dr. Rajesh Yadav (IC, DIBDO)
 Amarajit Singh (Asst Dir, DCPW)
 Jayasankar M.N (AVC-IT, CRPF)
 Anilkamboj (SI/Tech-CRPF)
 S.P. Singh (Asst Comm, RSF)
 R.K. Kithbhare (AVC-Comm, SSB)
 Pardeep Kumar Yadav (AVC-ITBP)
 Sunil Singh (SI/Tech-ITBP)
 S.M.H. Hasnain (Dir-IT, CRPF)
 Jagjit Singh (TD, NIC)
 Alok Nath Choudhary (TD, NIC)
 D.K. Khan (TD, NIC)
 V.V. Ramana (TD, NIC)
 Dr. Rajesh Yadav (IC, DIBDO)
 Amarajit Singh (Asst Dir, DCPW)
 Jayasankar M.N (AVC-IT, CRPF)
 Anilkamboj (SI/Tech-CRPF)
 S.P. Singh (Asst Comm, RSF)
 R.K. Kithbhare (AVC-Comm, SSB)
 Pardeep Kumar Yadav (AVC-ITBP)
 Sunil Singh (SI/Tech-ITBP)

154

<p>2.1.5</p> <p>Intrusion Prevention System (IPS)</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>S.M.Hasnain (DD-IT-CRPP)</p> <p>Jagjit Singh (TD, NIC)</p>
<p>2.1.3</p> <p>Anti-virus</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Alok Raj Choudhary (DD, NIC)</p> <p>D.H.Khan (SPD, NIC)</p>
<p>2.1.4</p> <p>URL Filtering</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>M.A.Ramana (TD, NIC)</p> <p>Purnaba Kanti Sharma (TD, NIC)</p>
<p>2.1.5</p> <p>Traffic Shaping</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Dr. Rajesh Yadav (CC, DIPP)</p> <p>Kapil (SSA, IPRND)</p>
<p>2.1.6</p> <p>Virtual Private Network</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Anurag Singh (AC-IT, IPR)</p> <p>D.K. Singh (IT, IPR)</p>
<p>2.1.7</p> <p>Application Control</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>E. Assul D. D. P. W.</p> <p>Kulwinder Singh (Asst. Tech. IPR)</p>
<p>2.2</p> <p>High-Availability of MFSAs device</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Jayantkar M.N (AC-IT, CRPP)</p> <p>Anil Kapoor (DD-IT, IPR)</p>
<p>2.2.1</p> <p>All MFSAs functions mentioned at point no. 2.1 must work in High-Availability mode.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Anil Kapoor (SITech-IPR)</p> <p>Mai, Piyush Elaura (NSO)</p>
<p>2.3</p> <p>The MFSAs license must not have restriction on number of users or IP addresses for all MFSAs functions / modules mentioned in point no. 2.1.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>S.P. Singh (Inspe, Comg, BSR)</p> <p>Ashok Sharma (Asst. Comm, SSB)</p>
<p>2.4</p> <p>The device must be deployable in routing mode.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>R.K. Kumbhare (AC-Comm, SSB)</p> <p>Sunil Singh (SITech, IPR)</p>
<p>2.5</p> <p>The device must support the following routing protocols:</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Pardeep Kumar Yadav (AC-ITPR)</p>

BGP

153

2.5.2	OSPF	The device must be deployable in bridge (transparent) mode.	View in Technical guide and verify features using Console / Web console	S.M. Hasnain (D/C-IT-CRPF)	Jagjit Singh (TD, NIC)
2.6	2.6.1	All MFSA modules must work in bridge mode except point no. 2.1.6.	View in Technical guide and verify features using Console / Web console	Alok Kati Choudhary (TD, INR)	D. BLKhan (TD, NIC)
2.6	2.6.2	BGP protocol packets must pass through transparently in bridge mode.	View in Technical guide and verify features using Console / Web console	V.K. Ramana (TD, NIC)	I. Shriha Jayoti Sharma (TD, NIC)
2.6	2.6.3	Must support multicast packets in bridge mode.	View in Technical guide and verify features using Console / Web console	Dr. Rajesh Yadav (ICG, DRDO)	K. Rajit (C&A) (PR&CH)
2.7		The device must support multiple network subnets on a physical network interface.	View in Technical guide and verify features using Console / Web console	Anuragjit Singh (E. Ass. Dir, DCI&W)	D.K. Singh (L2 IT-IT, CRPF)
2.8		Video & Voice support:	View in Technical guide and verify features using Console / Web console	Jayasankar M.N (AVC-IT, CRPF)	Kulvinder Singh (Insp. Tech-CRPF)
2.9	2.8.1	Must be session-aware to inspect various Video & voice protocols, such as, H.323 and Session Initiation Protocol (SIP) protocols.	View in Technical guide and verify features using Console / Web console	Anil Kamboj (SI/Tech-CRPF)	Abhil Kajpuri (D/C-IT, ISB)
2.9		The device must support Dual-Stack IPv4 and IPv6 for all MFSA modules.	View in Technical guide and verify features using Console / Web console	S.P. Singh (Insp/C-opp-SSB)	Maj. Piyush Tilaga (NSC)
2.10		Logging and Monitoring:	View in Technical guide and verify features using Console / Web console	R.K. Kumbhare (AVC-Comm, SSB)	Ashok Sharma (Insp/Comm, SSB)
2.10	2.10.1	It must be able to send logs to external syslog server and MFSA Log analysis Solution.	View in Technical guide and verify features using Console / Web console	Pardeep Kuthar Yadav (AVC-IT&B)	Sumit Singh (S&IT, ISB)

182

<p>2.11 Device Management:</p>	<p>View in Technical guide and verify features using Console / Web console</p>																										
<p>2.11.1 The device must be manageable from Centralised Management Solution.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>S.M. Hasnain (DIG-IT, CRPP)</p>																									
<p>2.11.2 The device must support role based administration.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Alola Kar Choudhary (DIG, NIC)</p>																									
<p>2.11.3 The device must support management over secure channel.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Dr Rajesh Yadav (DIG, DRPO)</p>																									
<p>2.11.4 The device must restrict management from specified IP addresses / networks.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Antarajit Singh (Asst. Dir. DRPW)</p>																									
<p>2.11.5 The device must support AAA authentication</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Jayasankar M.N (Asst. Dir. CRPP)</p>																									
<p>2.12 Certifications:</p>	<table border="1"> <thead> <tr> <th>FAI #</th> <th>ISO</th> <th>Checkmark</th> <th>ICSA Labs</th> <th>NSS Labs</th> </tr> </thead> <tbody> <tr> <td>2.12.1</td> <td>15408</td> <td></td> <td></td> <td></td> </tr> <tr> <td>2.12.1.1</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2.12.1.2</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2.12.1.3</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	FAI #	ISO	Checkmark	ICSA Labs	NSS Labs	2.12.1	15408				2.12.1.1					2.12.1.2					2.12.1.3					<p>Kulvinder Singh (Asst. Tech. CRPP)</p>
FAI #	ISO	Checkmark	ICSA Labs	NSS Labs																							
2.12.1	15408																										
2.12.1.1																											
2.12.1.2																											
2.12.1.3																											
<p>2.13 Warranty & Software subscriptions:</p>	<p>From tender document</p>	<p>Anil Kumar (SITech-TRPP)</p>																									
<p>2.13.1 Five years on-site comprehensive warranty support</p>	<p>From tender document</p>	<p>S.P. Singh (Asst. Dir. CRPP)</p>																									
<p>2.13.2 Five years software subscription support</p>	<p>From tender document</p>	<p>Mej. Divyash Tripathi (INSCL)</p>																									
		<p>Anshu Sharma (Asst. Dir. CRPP)</p>																									
		<p>Pardeep Kumar Yadav (Asst. TRPP)</p>																									
		<p>Samir Singh (SITech-TRPP)</p>																									

(18)

(C-100)

3.	FIREWALL Must be a Stateful packet inspection firewall. 3.1. 3.2. Firewall module must support security policies (firewall rules) based on: 3.2.1. IP address 3.2.2. Network subnet 3.2.3. Protocol (TCP, UDP, ICMP, etc.) 3.2.4. Services 3.2.5. Time 3.2.6. User-group 3.3. Must have provision to create local users on the device to support user based security policies 3.4. Must integrate with the following third-party authentication services to support user based security policies:	S.M Hasnain (DIG-IT, CRPF) Alok Ran Choudhary (IT, NIC) V.P. Ramana (IT, NIC) Dr. Rajesh Yadav (CCG, DRDO) Anurajit Singh (Asst. Dir. DCPW) Jayasankar M.N (AVC-IT, CRPF) Anil Kambhoj (SI/Tech-CRPF) S.P. Singh (Asst. Comd-BSF) R.K. Kumbhare (AVC-Comm, SSIB)	Jagjit Singh (IT, NIC) D.J. Khan (SI/IT, NIC) Dhruva Jyoti Sharma (IT, NIC) Keptil (NSA, IPR&D) D.C. Singh (IT, CRPF) Kulwinder Singh (Asst. Tech-CRPF) Anil Kumbhoj (SI/Tech-CRPF) Maj. Pankaj Tripathi (NSC) Ashok Sharma (Asst. Comd, SSIB)	Pardeep Kumar Yadav (AVC-ITIB)	Sumit Singh (SI/IT, CRPF)
----	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------	------------------------------

<p>3.4.1. LDAP</p> <p>3.4.2. Windows Active Directory</p>	<p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p>	<p>S.M Hasnain (DCC-IT-CRPP)</p> <p>Alor Raza Choudhary (ITD-NIC)</p> <p>Jagjit Singh (ITD-NIC)</p> <p>D.H.Khan (ITD-NIC)</p>
<p>3.5. Network Address Translation (NAT): Must support the following:</p> <p>3.5.1. Dynamic NAT</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Dr. Rajesh Yadav (CCO, DIRDO)</p> <p>Dhruva Avasth Sharma (ITD-NIC)</p>
<p>3.5.2. Static NAT</p> <p>3.5.3. PAT</p>	<p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p>	<p>Amarajit Singh (ASST.DIR, DE.PWA)</p> <p>D.K.Singh (DCC-IT-CRPP)</p>
<p>3.5.4. No-NAT (traffic should pass without IP address translation)</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Jayasankar M.N (ASST.DIR, CRPP)</p> <p>Kulwinder Singh (Asst/tech-ITPP)</p>
<p>3.5.5. Policy based source and destination NAT</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Anil Kamboj (SIT/tech-CRPP)</p> <p>Anil Rajput (ASST-IT/BSF)</p>
<p>4. INTRUSION PREVENTION SYSTEM (IPS)</p>		
<p>4.1. The IPS must be able to detect and respond (block, notify) to any malicious activity.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>S.P. Singh (Asst/Comm/BSF)</p> <p>R.K. Kumbhare (ASST-Comm, SSBI)</p> <p>Atul Prakash Tripathi (ASST)</p> <p>Ashok Sharma (Asst Comm, SSBI)</p>
<p>4.2. Must be possible to configure traffic-direction based IPS policies.</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p>Pardeep Kumar Yadav (ASST-IT/BSF)</p> <p>Sunil Singh (SIT/IT/BSF)</p>

(149)

4.3	Must support creation of user-defined signatures.	View in Technical guide and verify features using Console / Web console	S.M. Hasnain (DIG-IT, CRPF) Jagjit Singh (ID, NIC)
4.4	IPS must support exemption of traffic inspection for: 4.4.1. Specific IP addresses	View in Technical guide and verify features using Console / Web console	Alok Raj Choudhary (IT, NIC) D.H. Khan (ASSTD, NIC)
4.5	4.5.1. Networks (source and destination separately)	View in Technical guide and verify features using Console / Web console	V.P. Ramana (ID, NIC) Dhruvrajyoti Sharma (ID, NIC)
4.5	Must be possible to block / allow files based on: 4.5.1. File names	View in Technical guide and verify features using Console / Web console	Dr. Rajesh Yadav (TCC, DRDO)
4.5	4.5.2. File extensions	View in Technical guide and verify features using Console / Web console	Amarajit Singh (Asstt. Dir, DCPW)
4.5	4.5.3. File types	View in Technical guide and verify features using Console / Web console	Jayasankar M.N. (AC-IT, CRPF)
4.6	Day Zero protection.	View in Technical guide and verify features using Console / Web console	Kulwinder Singh (Asstt. Tech-CRPF)
4.7	Identify & Block DoS & DDoS, Sync flagged & encrypted attacks.	View in Technical guide and verify features using Console / Web console	Anil Kamboj (SI/Tech-CRPF)
4.8	Custom Signature Support.	View in Technical guide and verify features using Console / Web console	S.P. Singh (Asstt. Comm, NSP) R.K. Kumbhare (AC-Comm, SSIB)
			Manoj Prakash Thakur (NSP) Ashok Sharma (Asstt. Comm, SSIB)
			Pardeep Kumar Yadav (AC-IT/IB) Sumit Singh (SI/Tech-IB)

(Page 2)

4.9	Should defend & monitor against worms, virus, Trojan	View in Technical guide and verify features using Console / Web console	S.M.Hasnani (DD-IT-CRPP)	Ajayit Singh (DD-SP)
4.10	Role based access to various IPS Policies.	View in Technical guide and verify features using Console / Web console	A.P.Srinivaschoudhary (DD-IT-CRPP)	D.H.Khan (DD-IT-CRPP)
5.	ANTIVIRUS	View in Technical guide and verify features using Console / Web console	V.T.J.Ramanna (DD-NIC)	Dhruva Jyoti Sharma (DD-NIC)
5.1.	Gateway Antivirus must provide real-time protection of viruses, worms, Trojans and other malicious code (like spyware, adware, etc.) at the gateway for SMTP, POP3, IMAP, HTTP, HTTPS, FTP & IM traffic in both directions.	View in Technical guide and verify features using Console / Web console	Dr. Rakesh Yadav (CCG-DRPD)	Kapil (SSA-BRCPD)
6.	URL FILTERING	View in Technical guide and verify features using Console / Web console	Amarajit Singh (ASST.DIR-DCPW)	D.K.Singh (DD-IT-CRPP)
6.1.	URL filtering must work for HTTP and HTTPS traffic	View in Technical guide and verify features using Console / Web console	Jayasankar M.N (AD-IT-CRPP)	Kulwinder Singh (DD-IT-CRPP)
6.2.	The following security related URL categories must be supported in addition to the other categories	View in Technical guide and verify features using Console / Web console	Anil Kamboj (SITech-CRPP)	Anil Kamboj (DD-IT-CRPP)
6.2.1.	BOTNETS	View in Technical guide and verify features using Console / Web console	S.P.Singh (DD-IT-CRPP)	Naji (NSK)
6.2.2.	Malicious sites	View in Technical guide and verify features using Console / Web console	R.K.Kanbhare (AD-COM-SSIP)	Ashok Sharma (DD-IT-CRPP)
6.2.3.	Phishing sites	View in Technical guide and verify features using Console / Web console	Pankaj Kumar Yadav (AD-ITIP)	Sunil Singh (SITech-CRPP)
6.2.4.	SPAM sites	View in Technical guide and verify features using Console / Web console		
6.2.5.	HACKING	View in Technical guide and verify features using Console / Web console		
6.2.6.	Proxy avoidance / remote proxy	View in Technical guide and verify features using Console / Web console		
6.2.7.	P2P file sharing	View in Technical guide and verify features using Console / Web console		
6.3.	URL filtering must be possible for specified:	View in Technical guide and verify features using Console / Web console		
6.3.1.	IP address	View in Technical guide and verify features using Console / Web console		
6.3.2.	Network subnet	View in Technical guide and verify features using Console / Web console		

147

6.3.3.	User-group	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> S.M. Hasain (DIG-IT, CRPF)</p> <p><i>[Signature]</i> Ajit Singh (ITD, NIC)</p> <p><i>[Signature]</i> Alok Choudhary (ITD, NIC)</p> <p><i>[Signature]</i> Dhruba Jyoti Sharma (ITD, NIC)</p> <p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.4.	Must be possible to block / allow		<p><i>[Signature]</i> Jagjit Singh (ITD, NIC)</p> <p><i>[Signature]</i> D.H. Khan (STH, NRC)</p> <p><i>[Signature]</i> D.K. Singh (L-16-IT-CRPF)</p> <p><i>[Signature]</i> Kulwinder Singh (Inspr/Tech-CRPF)</p> <p><i>[Signature]</i> M.J. Pooash Filafra (NSC)</p> <p><i>[Signature]</i> Ashok Sharma (Inspr/Comm, SSB)</p>
6.4.1.	URLs based on categories.	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.4.2.	Unrated sites.	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.4.3.	User-defined URLs.	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.5.	Must have provision to block / allow:		<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.5.1.	Web based chat traffic	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.5.2.	Peer to peer traffic	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.5.3.	Voice traffic	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.5.4.	Video traffic	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.6.	The solution must be able to block sites containing:		<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.6.1.	Spywares	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>
6.6.2.	Adwares	View in Technical guide and verify features using Console / Web console	<p><i>[Signature]</i> Dr. Rajesh Yadav (TCC, DRDO)</p> <p><i>[Signature]</i> Amarajit Singh (E- Assn. Dir. DCPW)</p> <p><i>[Signature]</i> Jayantkar M.N. (AVC-IT, CRPF)</p> <p><i>[Signature]</i> Anil Kamboj (SI/Tech-CRPF)</p> <p><i>[Signature]</i> S.P. Singh (Inspr/Gmg/BST)</p> <p><i>[Signature]</i> R.K. Kumbhare (AVC-Comm, SSB)</p>

146

<p>6.6.3. Malwares</p> <p>6.7. Must have configurable options to allow/deny access to web sites when the URL rating service is unavailable</p>	<p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p>	<p><i>Aravind</i></p> <p>S.M.Hasnain (Dir-IT-CRPF)</p> <p>Jagjit Singh (TD, NIC)</p> <p>A.O.Choudhary (Dir, NIC)</p> <p>D.H.Khan (STD, NIC)</p>
<p>7. TRAFFIC SHAPING</p> <p>7.1. Must be possible to enable Traffic Shaping (rate limiting) for specified:</p> <p>7.1.1. IP address</p> <p>7.1.2. Network subnet</p> <p>7.1.3. Services</p>	<p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p>	<p><i>Aravind</i></p> <p>Dr Rajesh Yadav (Tech. Dir,PO)</p> <p>Kapil (SSA,ITP&D)</p> <p>Amrajit Singh (Dir-IT-CRPF)</p> <p>D.K.Singh (Dir-IT-CRPF)</p> <p>Dhruva Jyoti Sharma (TD, NIC)</p>
<p>7.2. Must be possible to configure Guaranteed bandwidth for specified:</p> <p>7.2.1. IP address</p> <p>7.2.2. Network subnet</p> <p>7.2.3. Services</p>	<p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p> <p>View in Technical guide and verify features using Console / Web console</p>	<p><i>Aravind</i></p> <p>Anil Kamboj (SI/Tech-CRPF)</p> <p>Anil Rajput (Dir-IT-CRPF)</p> <p>Kulvinder Singh (Asst. Tech-Dir)</p> <p>Maj. Piyush Tiwari (NSO)</p> <p>Ashok Sharma (Asst. Comm. SSB)</p>
<p>7.3. Must be possible to configure Maximum bandwidth for specified:</p> <p>7.3.1. IP address</p>	<p>View in Technical guide and verify features using Console / Web console</p>	<p><i>Aravind</i></p> <p>Parddeep Kumar Yadav (Asst. Dir,IT)</p> <p>Smit Singh (Supt. Dir,IT)</p>

148

7.3.2. Network subnet	View in Technical guide and verify features using Console / Web console	S.M. Hasnain (DIG-IT, RPF)	Jagjit Singh (ID, NIC)
7.3.3. Services	View in Technical guide and verify features using Console / Web console	Alok Kar Choudhary (ID, NIC)	Jagjit Singh (ID, NIC)
8.	VIRTUAL PRIVATE NETWORK (VPN)	V.K. Kamana (ID, NIC)	Alok Kar Choudhary (ID, NIC)
8.1.	The device must support IPSEC VPN protocol.	Dr. Rajesh Yadav (CCG, DRDO)	Dhruva Jyoti Sharma (JIS, IIT)
8.2.	The device must support site to site VPN	Amarajit Singh (ASST.Dr, DCPW)	Dr. Rajesh Yadav (CCG, DRDO)
8.3.	The device must support remote-client VPN. Must include client licenses, if any, for the number of users mentioned in the technical specifications of the item.	Jayasankar M.N (AVC-IT, CRPF)	Dr. Rajesh Yadav (CCG, DRDO)
8.4.	The device must scan all VPN traffic for malicious content.	Anil Kamboj (SI/Teob-CRPF)	Dr. Rajesh Yadav (CCG, DRDO)
9.	APPLICATION CONTROL	Kulvinder Singh (Insp Tech-CRPF)	Dr. Rajesh Yadav (CCG, DRDO)
9.1.	Must discover applications automatically and enable application policy controls independent of port and protocol.	S.P. Singh (Insp/Coym, BSF)	Anil Kamboj (SI/Teob-CRPF)
9.2.	The device must be able to allow / deny applications based on:	R.K. Kumbhare (AVC-Comm, SSB)	Maj. Piyush Thapa (INSCT)
9.2.1.	Specified users	Pardeep Kumar Yadav (AVC-ITBP)	Ashok (Akarma) (Insp/Comm, SSB)
9.2.2.	Specified user groups	Pardeep Kumar Yadav (AVC-ITBP)	Smit Singh (SI/Teob-CRPF)

144

9.2.3	Specified user groups with exceptions	View in Technical guide and verify Features using Console / Web console	
9.2.4	Specified source IPs	View in Technical guide and verify features using Console / Web console	
9.2.5	Specified source Networks	View in Technical guide and verify Features using Console / Web console	
9.3	The device must identify and control Web 2.0 applications	View in Technical guide and verify features using Console / Web console	
5. No.	SPECIFICATION FOR MFSA LOG ANALYSIS SOLUTION	Trial Directive	
1.	Specify:		
1.1.	Item No.		
1.2.	OIM	View in Technical guide and verify same on physical device	
1.3.	Model	View in Technical guide and verify same on physical device	
1.4.	Rack space (1U, 2U, etc.)	View in Technical guide and verify same on physical device	
1.5.	Power requirement (in Watts)	View in Technical guide and verify same on physical device	
2.	Must be accessible through GUI.	View in Technical guide and verify same by accessing through interface	
3.	Must be accessible over secure channel.	View in Technical guide and verify same by accessing on secure channel (Https)	

S.M. Hasnain
(DIG-IT, CRPP)

Jagjit Singh
(TD, NIC)

Aditya Choudhary
(TD/NIC)

Dhruva Jyoti Sharma
(S/D, NIC)

Dhruva Jyoti Sharma
(TD, NIC)

Dhruva Jyoti Sharma
(S/D, NIC)

Dr. Rajesh Yadav
(ICG, DRDO)

Kapil
(SSA, APRAK)

Amarjit Singh
(E-Assist, Dir, DCPW)

D.K. Singh
(216-4T, CRPP)

Jayasankar M.N
(AVC-4T, CRPP)

Kulvinder Singh
(Insp/tech-CRPP)

Anil Kamboj
(SI/tech-CRPP)

Anil Kamboj
(402-4T, CRPP)

S.P. Singh
(Insp/Comm, CRPP)

Maj. Piyush Thakra
(INS)

R.K. Kamthare
(AVC-Comm, SSIR)

Ashok Sharma
(Insp/Comm, SSIR)

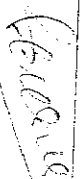

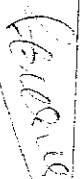

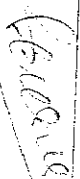

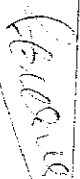

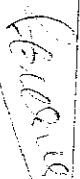


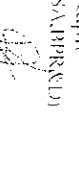
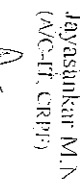
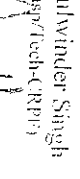
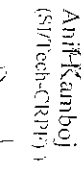
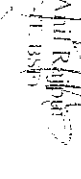
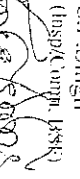

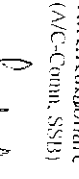
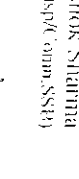
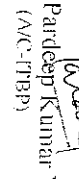
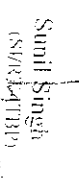
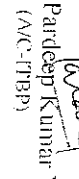
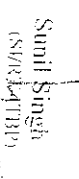
Paruldeep Kumhar
(AVC-ITIRP)

Shruti Singh
(SIR/CRPP)

143


4.	A single Log Analysis solution must support / he	<p>4.1. 100 or more MFSA devices</p> <p>4.2. Storage space of 2 TB or more</p> <p>4.3. RAID 5 redundancy</p> <p>4.4. Rack mountable</p> <p>4.5. 5000 Events Per Second (EPS)</p> <p>Must have provision to view and analyze real-time alerts from all MFSA devices.</p> <p>Drilldown facility must be available for alert monitoring.</p> <p>Must generate the following reports:</p> <p>7.1. Attack reports</p> <p>7.2. Bandwidth usage reports</p> <p>7.3. Source IP / destination IP reports</p> <p>7.4. Source network / destination network reports</p>	<p>View in Technical guide and verify same from console / management interface</p> <p>View in Technical guide and verify same from console / management interface</p> <p>View in Technical guide and verify same from console / management interface</p> <p>View in Technical guide and verify same from console / management interface</p> <p>View in Technical guide and verify same from console / management interface</p> <p>View in Technical guide and verify same from console / management interface</p> <p>View in Technical guide and verify same from console / management interface by forwarding log from other devices</p> <p>View in Technical guide and verify same from console / management interface for various alerts</p> <p>View in Technical guide and verify same from console / management interface by generating reports</p> <p>View in Technical guide and verify same from console / management interface by generating reports</p> <p>View in Technical guide and verify same from console / management interface by generating reports</p> <p>View in Technical guide and verify same from console / management interface by generating reports</p>	<p>S.M.Hashmi (DIG/IT, CRPF)</p> <p>Dr Rajesh Yadav (ICG, DRDO)</p> <p>V.P.T Ramana (FD, NIC)</p> <p>Dr Rajesh Yadav (ICG, DRDO)</p> <p>Amanjit Singh (Asstt Dir, DCPAW)</p> <p>Jayasankar M.N (AC/IT, CRPF)</p> <p>Anil Kamboj (SI/Tech-CRPF)</p> <p>S.P. Singh (Asstt Comm, ISB)</p> <p>R.K. Kumbhare (AC-Comm, SSB)</p> <p>Pardip Kumar Yadav (AC/ITBB)</p> <p>S.M. Hashmi (IT, NIC)</p> <p>Dr H. Khan (G.D, NIC)</p> <p>Dhruva Avon Sharma (FD, NIC)</p> <p>Kapil (SSA, IRR&D)</p> <p>D.K. Singh (LT-IT, CRPF)</p> <p>Kulwinder Singh (Asstt Tech, CRPF)</p> <p>Anil Kapil (Asstt Tech, CRPF)</p> <p>Maj Pankaj Tiwari (NSA)</p> <p>Ashok Sharma (Asstt Comm, SSB)</p> <p>Sonil Singh (Asstt Comm, SSB)</p>
----	--------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


142


7.5. User based reports	View in Technical guide and verify same from console / management interface by generating reports	 S.M. Hasnain (DIG-IT, CRPP)  Jagjit Singh (TD, NIC)
7.6. Service based reports	View in Technical guide and verify same from console / management interface by generating reports	 S.M. Hasnain (DIG-IT, CRPP)  Jagjit Singh (TD, NIC)
7.7. (URL) based reports	View in Technical guide and verify same from console / management interface by generating reports	 S.M. Hasnain (DIG-IT, CRPP)  Jagjit Singh (TD, NIC)
7.8. Access or Denied reports	View in Technical guide and verify same from console / management interface by generating reports	 S.M. Hasnain (DIG-IT, CRPP)  Jagjit Singh (TD, NIC)
7.9. User-defined reports	View in Technical guide and verify same from console / management interface by generating reports	 S.M. Hasnain (DIG-IT, CRPP)  Jagjit Singh (TD, NIC)
8. The solution must have provision to export log of a particular device as a text file for the specified period without any restriction on number of log entries or the size of the log file	View in Technical guide and verify same from console / management interface by exporting logs to other format	 Amarjit Singh (E- Assst. Dir. (DCTPW))  D.K. Singh (E/IT-IT, CRPP)
9. The solution must have configurable option to schedule the report generation.	View in Technical guide and verify same from console / management interface by generating reports on schedule based	 Jayasankar M.N (AG-IT, CRPP)  Kulwinder Singh (Asst/Tech-CRPP)
10. Must support sending the scheduled reports to the designated email addresses.	View in Technical guide and verify same from console / management interface by sending report to designated email	 Anil Kamboj (Sr/Tech-CRPP)  Anil Rajput (DVC-IT, ISSP)
11. Role based access for the log analyzer:	View in Technical guide and verify same from console / management interface granting role to user	 S.P. Singh (Asst/Comm, ISSP)  Manoj Prakash Tripathi (ISSP)
11.1. Must be possible to allow a given user to analyze the logs of one or more MFSA devices.	View in Technical guide and verify same from console / management interface granting role to user	 R.K. Kumbhare (AC-Comm, SSB)  Ashok Sharma (Asst/Comm, SSB)
11.2. Must support multiple roles like administrator, operator etc for the log analyzer.	View in Technical guide and verify same from console / management interface granting role to user	 Pardeep Kumar Yadav (AC-ITPP)  Sunil Singh (SVR-ITPP)
11.3. Remote access to the log analyzer must be possible from specific IP addresses / subnets only.	View in Technical guide and verify same from console / management interface by setting IP access	 Pardeep Kumar Yadav (AC-ITPP)  Sunil Singh (SVR-ITPP)


141


12.	Warranty & Software subscription:	
12.1.	Five years on-site comprehensive warranty support	View in Tender document
12.2.	Five years software subscription support.	View & verify in tender document
12.3.	Management Console should support CLI/GUI	View & verify in tender document


 S.M. Hashain
 (DIG-IT, CRPF)


 Jagjit Singh
 (TD, NIC)

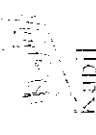
 Alok Kari Choudhary
 (TD, NIC)


 D.K. Khan
 (STD, NIC)

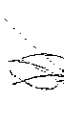
 V.T.M. Ramana
 (TD, NIC)


 Dhruba Jyoti Sharma
 (JD, NIC)


 Dr. Rajesh Yadav
 (TCG, DRDO)


 Kapil
 (SSA, BPR&D)


 Amarajit Singh
 E.Asstt.Dir, DCPW)


 D.K. Singh
 (2 I/C-IT, CRPF)


 Jayasankar M.N
 (A/C-IT, CRPF)


 Kulwinder Singh
 (Insp/Tech-CRPF)


 Amil Kamboj
 (SI/Tech-CRPF)


 S.P. Singh
 (Insp/Comm, BSF)


 Maj Piyush Tiwari
 (NSG)

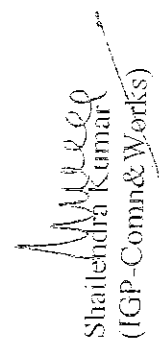
 R.K. Kumbhare
 (A/C-Comm, SSB)

 Ashok Sharma
 (Insp/Comm, SSB)

 Pardeep Kumar Yadav
 (A/C-ITBP)

 Sunil Singh
 (SI/RT-ITBP)

 Anil Rajput
 (D/C-IT, BSF)

 Shaitendra Kumar
 (IGP-Comm & Works)

APPROVED/NOT-APPROVED

 Pzakash Mishra
 DG CRPF