No. M.V-12/2012-13-DA.IV.IT 84/
भारत सरकार/Government of India
मंत्री प्रमुख/Secretary
मंत्री घर/Ministry of Home Affairs
पुलिस आयुक्तीकरण प्रभाग /Police Modernization Division
संभारण-1 छोटा /Prov.1 Desk

26, Man Singh Road, Jaisalmer House,
New Delhi, dated the 24th 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,

(M. K. Chahar)
Under Secretary to the Govt. of India

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

1. Must support the following parameters with CPU utilization < 50% |

<table>
<thead>
<tr>
<th>No. of Concurrent Users</th>
<th>Throughput (in Mbps)</th>
<th>Network Ports (10 / 100 / 1000 Mbps)</th>
<th>Concurr June 2021ents connect 10 K on or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>250</td>
<td>1000</td>
<td>500</td>
<td>Minimum 6 Nos. 2 Lakhs or more</td>
</tr>
</tbody>
</table>

MFSA Model-1 HA: MFSA device for High-Availability of MFSA Model-1

MFSA Log Analysis solution

S.M.Hasnain (DIG-IT,CRPF) Jagjit Singh (TD, NIC) Ashok 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) Amarjit 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/JT, BSF) S.P.Singh (Insp/Comm, BSF)
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 Shaping
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 Rana-Chaudhary (TD, NIC)
D.P.Khan (STD, NIC)
V.T.T Ramana (TD, NIC)

Dhrub Jyoti Sharma (TD, NIC)
Dr Rajesh Yadav (TCG, DRDO)
Kapil (SSA,BPR&O)
Amerajit Singh (E,Asstt.Dir, DCPW)
D.K.Singh (2/C-IT, CRPF)

Jayasanker M.N (A/C-IT, CRPF)
Kulwinder Singh (Insp/tech-CRPF)
Anil Kamboj (SI/tech-CRPF)
Anil Raipur (D/C-IT, BSF)
S.P.Singh (Insp/Comm, BSF)

Maj Piyush Tilaga (NSG)
R.K.Kumibhare (A/C-Comm, SSB)
Ashok Sharma (Insp/Comm, SSB)
Pardep Kumar Yadav (A/C-ITBP)
Sunit Singh (SI/RT4TBP)
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.

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:

<table>
<thead>
<tr>
<th>EAL4</th>
<th>ISO 15408 Checkmark</th>
<th>ICSCA Labs</th>
<th>NSS Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Firewall &amp; VPN modules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Antivirus module</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPS module</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
(TD, NIC)

Jagjit Singh
(TD, NIC)

Alok Rai Choudhary
(TD, NIC)

D.K. Khan
(STD, NIC)

V.T.T Ramana
(TD, NIC)

Dhruba Iyoti Sharma
(TD, NIC)

Dr Rajesh Yadav
(TCG, DRDO)

Kapil
(SSA, BPR&D)

Amarjit Singh
(E Asstt. Dir, DCPW)

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

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

Kulwinder Singh
(Inspt/ Tech-CRPF)

Anil Kambal
(SI/ Tech-CRPF)

Anil Rajput
(D/C-IT, BSF)

S.P. Singh
(Inspt/ Commn, BSF)

Maj Prashant Tilaga
(NSG)

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

Ashok Sharma
(Inspt/ Commn, SSB)

Pardeep Kumar Yadav
(A/C-ITBP)

Simi Singh
(SI/RT-ITBP)
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 policies.
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
4.8. Custom Signature Support.
4.9. Should defend & monitor against worms, viruses, Trojan
4.10. Role-based access to various IPS Policies.

S.M. Hasnain (DGP-IT, CRPF)
Jagjit Singh (TD, NIC)
Anil Kumar Choudhary (TD, NIC)
D.M. Khan (STD, NIC)
V.K. Ramana (TD, NIC)

Dhruba Jyoti Sharma (TP, NIC)
Dr. Rajesh Yadav (TCG, DRDO)
Kapil (SSA, BPR&D)
Amarajit Singh (E. Asstt. Dir, DCPW)
D.K. Singh (2 l/C-IT, CRPF)

Jayasankar M.N (A/C-IT, CRPF)
Kulwinder Singh (Insp/tech-CRPF)
Anil Kembaj (SI/tech-CRPF)
Anil Rajput (D/C-IT, BSF)
S.P. Singh (Insp/Comm, BSF)

Maj Pyyush Talaga (NSG)
R.K. Kumbhare (A/C-Comm, SSB)
Ashok Sharma (Insp/Comm, SSB)
Pardeep Kumar Yadav (A/C-ITBP)
Sunil Singh (SI/IT-ITBP)
5. **ANTIVIRUS**

5.1 Gateway Antivirus must provide real-time protection of viruses, worms, Trojan, 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

---

(Signatures and names of employees)
6.5.2 Adware
6.5.3 Malware

8.7. 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 independently 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.K. 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
(Inspect, Tech-CRPF)

Anil Kamboj
(SI/Tech-CRPF)

Anil Rajput
(D/C-IT, BSF)

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

Mai Pushpa
(INSGP)

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

Ashok Sharma
(Inspect/Comm, SSB)

Pardeep Kumar Yadav
(A/C-ITBP)

Sunit Singh
(SI/RPS-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

<table>
<thead>
<tr>
<th>S. No.</th>
<th>SPECIFICATION FOR MFSA LOG ANALYSIS SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Specify:</td>
</tr>
<tr>
<td>1.1.</td>
<td>Item No.</td>
</tr>
<tr>
<td>1.2.</td>
<td>OEM</td>
</tr>
<tr>
<td>1.3.</td>
<td>Model</td>
</tr>
<tr>
<td>1.4.</td>
<td>Rack space (1U, 2U, etc.)</td>
</tr>
<tr>
<td>1.5.</td>
<td>Power requirement (in Watts)</td>
</tr>
<tr>
<td>2.</td>
<td>Must be accessible through GUI.</td>
</tr>
<tr>
<td>3.</td>
<td>Must be accessible over secure channel.</td>
</tr>
<tr>
<td>4.</td>
<td>A single Log Analysis solution must support / be</td>
</tr>
<tr>
<td>4.1.</td>
<td>100 or more MFSA devices</td>
</tr>
<tr>
<td>4.2.</td>
<td>Storage space of 2 TB or more</td>
</tr>
<tr>
<td>4.3.</td>
<td>RAID 5 redundancy</td>
</tr>
<tr>
<td>4.4.</td>
<td>Rack mountable</td>
</tr>
<tr>
<td>4.5.</td>
<td>5000 Events Per Second (EPS)</td>
</tr>
<tr>
<td>5.</td>
<td>Must have provision to view and analyze real-time alerts from all MFSA devices.</td>
</tr>
<tr>
<td>6.</td>
<td>Drilldown facility must be available for alert monitoring.</td>
</tr>
<tr>
<td>7.</td>
<td>Must generate the following reports:</td>
</tr>
<tr>
<td>7.1.</td>
<td>Attack reports</td>
</tr>
<tr>
<td>7.2.</td>
<td>Bandwidth usage reports</td>
</tr>
<tr>
<td>7.3.</td>
<td>Source IP / destination IP reports</td>
</tr>
</tbody>
</table>

S.M.Hasnain (DIG-IT,CRPF)  Jagjit Singh (TD, NIC)  Alok Rai Choudhary (TD, NIC)  D.R.Khan (STD, NIC)  V.T.T Ramana (TD, NIC)
Dhruba Jyoti Sharma (TP, NIC)  Dr Rajesh Yadav (TCG, DRDO)  Kapil (SSA,BPR&D)  Amarajit Singh (E.Asst. 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 (0/C-IT, BSF)  S.P.Singh (Insp/Comm, BSF)
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 (DG-IT, CRPF)
Ingin 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/TCG, CRPF)

Jayasankar M.N. (A/C-IT, CRPF)
Kulwinder Singh (InsupTech-CRPF)
Anil Kamboj (SI/ITCRPF)
Anil Rajput (D/C-IT, BSF)
S.P. Singh (InsupComm, BSF)

Maj Piyush Tiwari (NSG)
R.K. Kumbhare (A/C-Comm, SSB)
Ashok Sharma (Insup Comm, SSB)
Pardeep Kumar Yadav (A/C-ITBP)
Sunit Singh (SI/RTP, ITBP)

Shailendra Kumar (IGP Comm & Work)

APPROVED/NOT APPROVED.

P.K. Mishra
DG CRPF
<table>
<thead>
<tr>
<th>S. No.</th>
<th>MFSA SPECIFICATION</th>
<th>Details</th>
<th>MFSA SPECIFICATION (Mandatory)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.1.</td>
<td>Throughput supported by the device (in Mbps)</td>
<td>GENERAL</td>
</tr>
<tr>
<td></td>
<td>1.1.1.</td>
<td>Firewall Throughput</td>
<td>The MFSA device must have the following Integrated functions / modules</td>
</tr>
<tr>
<td></td>
<td>1.1.2.</td>
<td>Firewall + IPS (All signatures enabled) Throughput</td>
<td>2.1.1.</td>
</tr>
<tr>
<td></td>
<td>1.1.3.</td>
<td>Firewall + IPS (All signatures enabled) + Antivirus Throughput (flow-based / proxy-based)</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td></td>
<td>1.2.</td>
<td>Concurrent Sessions supported with all modules enabled</td>
<td>Verify from product catalogue and match with supplied product</td>
</tr>
<tr>
<td></td>
<td>1.2.1.</td>
<td>New connections per second</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.3.</td>
<td>Rack space (1U/2U, etc.)</td>
<td>View in Technical guide and verify features</td>
</tr>
<tr>
<td></td>
<td>1.4.</td>
<td>Operating Voltage - 110-240V AC</td>
<td>View in Technical guide and verify features</td>
</tr>
<tr>
<td></td>
<td>1.5.</td>
<td>temperature - 5 to 40°C</td>
<td>View in Technical guide and verify features</td>
</tr>
<tr>
<td></td>
<td>1.6.</td>
<td>AC Frequency - 50/60 Hz</td>
<td>View in Technical guide and verify features</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>MFSA SPECIFICATION (Mandatory)</strong></td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>The device must support the following runtime protocols:</td>
<td>Use in Technical Guide and Very Learners</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use (Console / Web console)</td>
<td>View in Technical Guide and Very Learners</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View in Technical Guide and Very Learners</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use (Console / Web console)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View in Technical Guide and Very Learners</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use (Console / Web console)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View in Technical Guide and Very Learners</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The device must be deployable in runtime mode.

Installation in point no. 7.

1. NWSA Function modeled at point no. 7.

High-Viability of NWSA device.

\[ \text{Application Context} \]

\[ \text{Annual Plan Network} \]

\[ \text{Term Sheet} \]

\[ \text{Ink Plan} \]

\[ \text{Annual View} \]

\[ \text{Innovation Prevention System (IPS)} \]
| 2.6. | The device must be deployable in bridge (transparent) mode. |
|      | **2.6.1.** All MFSAs 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 MFSAs 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. |
### 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.

3.4. Must integrate with the following third-party authentication services to support user-based security policies:

<table>
<thead>
<tr>
<th>View in Technical guide and verify features using Console / Web console</th>
</tr>
</thead>
<tbody>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>Step</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>1.1</td>
</tr>
<tr>
<td>1.2</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2.1</td>
</tr>
<tr>
<td>2.2</td>
</tr>
<tr>
<td>2.3</td>
</tr>
<tr>
<td>2.4</td>
</tr>
<tr>
<td>2.5</td>
</tr>
<tr>
<td>2.6</td>
</tr>
<tr>
<td>2.7</td>
</tr>
</tbody>
</table>

Notes:
- It is possible to continue watching intrusion detection rules while in Technical and Vertx Features.
- The IPS must be able to detect and respond (block, notify) to malicious activities.
<table>
<thead>
<tr>
<th>Section</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>Must support creation of user-defined signatures.</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.4</td>
<td>IPS must support exemption of traffic inspection for:</td>
<td></td>
</tr>
<tr>
<td>4.4.1</td>
<td>Specific IP addresses</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Networks (source and destination separately)</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.5</td>
<td>Must be possible to block / allow files based on:</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.5.1</td>
<td>File names</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.5.2</td>
<td>File extensions</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.5.3</td>
<td>File types</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.6</td>
<td>Day Zero protection.</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.7</td>
<td>Identify &amp; Block DoS &amp; DDoS, Synt flagged &amp; encrypted attacks.</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>4.8</td>
<td>Custom Signature Support.</td>
<td>View in Technical guide and verify features using Console / Web console</td>
</tr>
<tr>
<td>6.3.3. User-group</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>6.4. Must be possible to block/allow</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.4.1. URLs based on categories.</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.4.2. Unrated sites.</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.4.3. User-defined URLs.</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.5. Must have provision to block/allow:</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.5.1. Web based chat traffic</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.5.2. Peer to peer traffic</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.5.3. Voice traffic</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.5.4. Video traffic</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.6. The solution must be able to block sites containing:</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.6.1. Spywares</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
<tr>
<td>6.6.2. Adwares</td>
<td>View in Technical guide and verify features using Console/Web console</td>
<td></td>
</tr>
</tbody>
</table>
7.5.2. Network subnet

7.5.3. 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

9.2.2. Specified user groups

View in Technical guide and verify features using Console / Web console.
<table>
<thead>
<tr>
<th>Physical Device</th>
<th>View in Technical Guide and Verify Same by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Requirement (in Watts)</td>
<td>1.2 Ohm (1.2, 1.0, etc.)</td>
</tr>
<tr>
<td>Back Splice (LC, 2U, etc.)</td>
<td>1.0 Ohm</td>
</tr>
<tr>
<td>Model</td>
<td>0.54 Ohm</td>
</tr>
<tr>
<td>From:</td>
<td>2.4 Ohm</td>
</tr>
</tbody>
</table>

**Solution**

**SPECIFICATION FOR MESA LOG ANALYSIS**

- Use Console / Web console
- View in Technical Guide and Verify features
- Use Console / Web console
- View in Technical Guide and Verify features
- Use Console / Web console
- View in Technical Guide and Verify features
- Use Console / Web console
- View in Technical Guide and Verify features

The device must identify and control Web 2.0 applications

Specified Source Networks

Specified Source IPs

Specified user groups with exceptions
A single Log Analysis solution must support / be

<table>
<thead>
<tr>
<th>4.1</th>
<th>100 or more MFSA devices</th>
<th>View in Technical guide and verify same from console / management interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>Storage space of 2 TB or more</td>
<td>View in Technical guide and verify same from console / management interface</td>
</tr>
<tr>
<td>4.3</td>
<td>RAID 5 redundancy</td>
<td>View in Technical guide and verify same from console / management interface</td>
</tr>
<tr>
<td>4.4</td>
<td>Rack mountable</td>
<td>View in Technical guide and verify same from console / management interface</td>
</tr>
<tr>
<td>4.5</td>
<td>5000 Events Per Second (EPS)</td>
<td>View in Technical guide and verify same from console / management interface</td>
</tr>
</tbody>
</table>

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
   View in Technical guide and verify same from console / management interface by generating reports

   7.2. Bandwidth usage reports
   View in Technical guide and verify same from console / management interface by generating reports

   7.3. Source IP / destination IP reports
   View in Technical guide and verify same from console / management interface by generating reports

   7.4. Source network / destination network reports
   View in Technical guide and verify same from console / management interface by generating reports
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>Remove access to the log analyzer must be possible</td>
</tr>
<tr>
<td>1.2</td>
<td>Then support multiple roles like administrator</td>
</tr>
<tr>
<td>1.1</td>
<td>The logs of one or more MSA devices</td>
</tr>
<tr>
<td>1.0</td>
<td>More based access for the log analyzer</td>
</tr>
<tr>
<td>1.0</td>
<td>Must support sending the scheduled reports to the designated email</td>
</tr>
<tr>
<td>0.9</td>
<td>The solution must have the capability to schedule the reports</td>
</tr>
<tr>
<td>0.8</td>
<td>The solution must have provision to export logs of a single or defined reports</td>
</tr>
<tr>
<td>0.7</td>
<td>Access of defined reports</td>
</tr>
<tr>
<td>0.6</td>
<td>Service based reports</td>
</tr>
<tr>
<td>0.5</td>
<td>Generated reports</td>
</tr>
<tr>
<td>0.4</td>
<td>Generated reports</td>
</tr>
<tr>
<td>0.3</td>
<td>Generated reports</td>
</tr>
<tr>
<td>0.2</td>
<td>Generated reports</td>
</tr>
<tr>
<td>0.1</td>
<td>Generated reports</td>
</tr>
</tbody>
</table>

Note: The image contains handwritten annotations and appears to be part of a larger document or presentation. The content seems to be related to network or system administration, focusing on logging and access control.
### Warranty & Software subscription:

<table>
<thead>
<tr>
<th>12.1. Five years on-site comprehensive warranty support</th>
<th>View in Tender document</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2. Five years software subscription support.</td>
<td>View &amp; verify in tender document</td>
</tr>
<tr>
<td>12.3. Management Console should support CLI/GUI</td>
<td>View &amp; verify in tender document</td>
</tr>
</tbody>
</table>

---

Approved/Not Approved:

Praaksh Mishra  
DG CRPF