Cyber Security Group
National Informatics Centre
Department of Information Technology

Firewall Rule Entry Request Form

(For Updating/Adding/Deleting a Rule*****)

Please Read Firewall Rule Entry Policy (PTO)

1. Name of the Group/Division :
2. Functionality & OS of the Server to be placed behind Firewall:
3. ## **Server's IP** number :
4. Rule Required on the Firewall to allow the Server to access outside systems:

From (## **Server's IP** number)	To (Destination IP number)	Service(s) to be accessed by the server (with reason)			Protocol (tcp / udp)	Permit for Time & Day						
		Name	Port(s)	Reason		From (Hrs)	To (Hrs)	Day(s) of week				
								M	T	W	T	
								F	S	S		

5. Rule Required on the Firewall to allow access from outside systems to the Server:

From (Source IP number)	To (## **Server's IP** number)	Service(s) to be provided by the server (with reason)			Protocol (tcp / udp)	Permit for Time & Day						
		Name	Port(s)	Reason		From (Hrs)	To (Hrs)	Day(s) of week				
								M	T	W	T	
								F	S	S		

6. Functionality offered by the Server is approved by competent authority: Yes/No
7. Server scanned for vulnerabilities** : Yes/No

NOTE: ## IP number of the Server to be placed behind the firewall (point 3, 4 & 5).

**** Use a separate sheet for each rule.***

***** Vulnerability scanner should be run for server before placing behind the firewall. Attach scan report and action taken.***

System Administrator details: Name:
Tel. No../ Intercom: E-Mail:

Signature of HoD with date:

Name & Designation of HoD:

Tel. No./Intercom: E-Mail:

Name & Signature of HoD (Cyber Security Group):

Comments :

Name & Signature of Firewall Administrator:

Firewall Rule Entry Policy

Systems to be installed behind the firewall shall conform to the following before they are physically connected to the network:

i. OS shall be installed and all relevant patches and hot fixes till date shall be applied without connecting to Internet.
ii. All unnecessary ports/services shall be closed/disabled.
iii. All unused accounts shall be disabled.
iv. Password policy shall be applied wherever applicable.
v. All accounts that are enabled shall have passwords assigned.
vi. System shall be scanned for vulnerabilities. CSG shall be approached for the same.
vii. All the vulnerabilities for services offered shall be fixed with the help of vendor or corresponding support division.
viii. All necessary precautions for the offered services, including ACL and audit procedures, shall be enforced on the server.
ix. Virus scan shall be done before moving the server behind the firewall.
x. Action taken report of vulnerabilities shall accompany the request form for installing system(s) behind the firewall.
xi. Patches for the above services will be applied as and when the software vendor for any future vulnerability releases them.

Note: **If the SERVER does not conform to any of the aforesaid points, the SERVER shall not be moved behind the Firewall as it could lead to network compromise.**

Example 1:

If the Server (say ***164.100.9.z*** that is behind the firewall) has ***to*** access a website (say ***20.30.40.50***) over ***http*** from ***10:00 A.M. to 5:00 P.M.*** on working days (i.e. ***Monday to Friday*** only), the point no. 4 has to be filled as shown under:

4. Rule Required on the Firewall to access from the Server to outside systems:

From (## **Server's IP** number)	To (Destination IP number)	Service(s) to be accessed by the server (with reason)			Protocol (tcp / udp)	Permit for Time & Day		
		Name	Port(s)	Reason		From (Hrs)	To (Hrs)	Day(s) of week
164.100.9. z	20.30.40.50	Web access	80 (http)	To update patches	tcp	10:00 HRS	17:00 HRS	Tick Monday to Friday

Example 2:

If an outside system ***(say 164.100.x.y)*** has ***to*** be allowed ***telnet*** service on Server (say ***164.100.9.z*** that is behind the firewall***)*** from ***10:00 A.M. to 5:00 P.M.*** on working days (i.e. ***Monday to Friday*** only), the point no. 5 has to be filled as shown under:

5. Rule Required on the Firewall to allow access from outside systems to the Server:

From (Source IP number)	To (## **Server's IP** number)	Service(s) to be provided by the server (with reason)			Protocol (tcp / udp)	Permit for Time & Day		
		Name	Port(s)	Reason		From (Hrs)	To (Hrs)	Day(s) of week
164.100.x.y	***164.100.9.z***	***telnet***	23	Telnet only from NIC domain	tcp	10.00 Hrs	17.00 Hrs	Tick Monday to Friday