SECURITY FOR WIDE AREA NETWORK OF BSNL

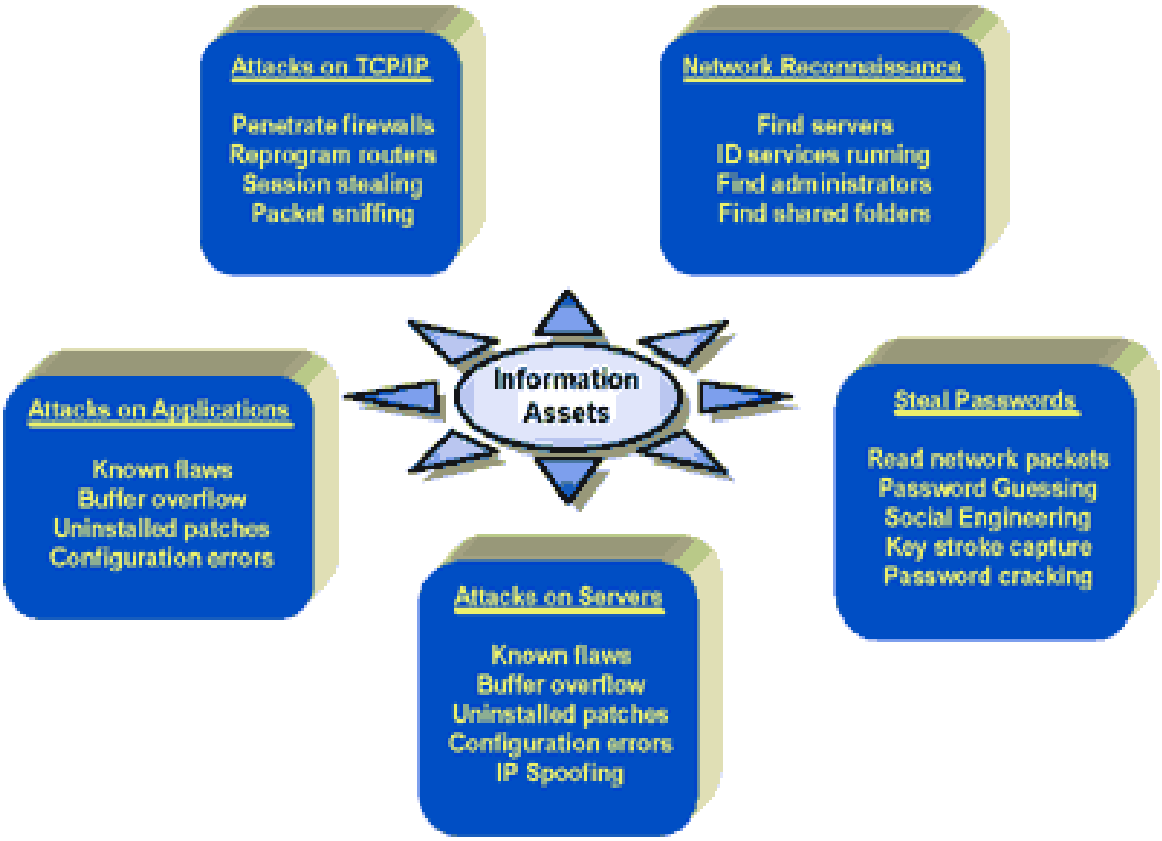
Vineet Mathur

GM(IT Project Circle)

Maintaining policies, procedures and adopting adequate security measures for a Information Network is gaining more and more importance due to the increasing dependence on the IT infrastructure for extending services to our customers as well as for office working. More and more data is being stored on computers, and it is very essential that the information provided by this data does not fall into wrong hands, is not corrupted or difficulty encountered in accessing it.

A tall building may be built in phases, but it's foundation is always built to take care of the ultimate height. Similarly, due care should be taken in respect of Network Security right at the initial stages when the network is being built up, even though the network itself may not seem so critical in the beginning. This will ensure that the various security aspects, like Policies and Procedures, as well as the requisite Hardware and Software become part of the network itself by the time the network becomes critical to our organization.

As the figure below illustrates, there are numerous vulnerabilities inside A Information network. Secure networking cannot be achieved without addressing these vulnerabilities.



Security is a Process, not a Product:

There is no out-of-the-box solution that will provide complete network protection. That is why there are so many complex components to a good security strategy. Some of those components are hardware or software products, some are simply written policies and guidelines, while others are user's and manager's mindsets and attitudes towards security.

The implementation of relevant hardware and software security solutions in the IT network should succeed and NOT preceed the framing of policies and guidelines, carrying out penetration and vulnerability tests to evaluate the status of the network.

The following are some of the various domains which should be considered while forming the policies and procedures. This is not an exhaustive list, and there can be further additions, if considered by the organization. Only those domains, which have a predominantly higher IT content have been taken up. Other domains, like Organization structure, Punitive actions have been referred to for completeness sake.

As and when the Wide Area Network and the resources kept on the WAN become critical, steps should be taken to carry out a Network Security Audit from a suitable vendor and take immediate steps to rectify any breaches found during the audit.

1. Security Organization Structure
2. Physical Security
3. Logical Access Controls
4. Password Security & Controls
5. Network & Telecommunication Security
6. Electronic Mail Security
7. Backup & Recovery
8. Incident Response and Management
9. Third Party Security
10. Internet access and security
11. Web server Security
12. Punitive Actions
13. Firewall Security
14. Virus Protection

PHYSICAL SECURITY

Swipe cards for access to the Server Room:

Swipe card should be used to provide required access to Server Room and its usage should be made mandatory. No unauthorized person should be able to gain access to the Server Room. Visitors should not be allowed entry inside the Server Room except with the written permission from authorized personnel.

Monitoring Access to Server Room:

A list of employees who are authorized to enter the Server Room (as approved by management) should be prepared and maintained. Except for these authorized employees, a 'Visitor's Register' should be maintained for tracking entry of all other personnel/ people.

Safety measures within the Server Room

No printers should be kept inside the Server Room. The entire stationary and other printer related consumable must not be kept in the server room.

LOGICAL ACCESS CONTROLS

Power-on passwords:

Power-on passwords should be used to prevent unauthorized personnel from starting the server. Only the Server Administrator should know this password. The password should be kept in a sealed envelope with the Head (IT).

Screen Saver Passwords:

Screen Saver Passwords should be used to prevent unauthorized personnel from accessing the server. Only the respective Server Administrator should know this password. The password should be kept in a sealed envelope with the Head (IT).

Creation of new users:

New users at operating systems, applications, database and network levels should be created based on formal authorizations by the respective functional heads.

Use of common user ID's:

Common user IDs should not be used. Common user IDs should not be issued for multiple users when it is technically feasible to provide individual IDs. In situations where a common ID is required, other than "inquiry-only " access, specific written permission should be taken from proper authority.

Sharing of user ID's:

There should be only one user ID common across multiple systems and applications for a single user. For example, for a user called 'USER' with user-id as 'USER', this user-id should be the same across the applications, operating systems network and other systems.

Disabling inactive user accounts:

User accounts that have been inactive for more than 30 days should be disabled. Systems Administrator should re-enable them only on the request of the specific user and where required, with the approval of the concerned department – head.

Disabling default user IDs:

Default user IDs shipped with all software should be disabled.

Deactivation of user ID:
If the wrong password is entered three times, the user-ID should be automatically deactivated and only the Database Administrator should carry out reactivation, after ascertaining genuine request or by the Systems Administrator (in absence of DBA)

System account suspension for failed login attempts:

Three successive failures should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset. The user should contact the Systems Administrator for getting the account unlocked. A history of all such failed attempts should be maintained and reviewed by the Systems Administrator periodically.

Inactivity time out:

The terminals should be deactivated after five minutes of inactivity. Additionally, screen saver passwords should be encouraged.

System to notify user of last login / logout:

Upon login, the user should be presented with date and time of last login and logout, along with contact information if they wish to report a discrepancy with their records.

User ID Management:

User ID creation form contains the information about the applications and privileges assigned application wise. A database maintaining this information about users and their access privileges should be updated every time a new user ID is created or terminated.

Use of Network Security Monitoring tools:

BSNL should deploy network security monitoring tools, to verify the compliance with the network policies and generate exception reports from the system to perform quick health-checks on network operations and management.

PASSWORD SECURITY AND CONTROLS

User passwords should remain confidential and not shared, posted or otherwise divulged in any manner.

Password Composition:

Passwords should consist of at least six alpha-numeric characters and should not contain the user's name or user-ID.

Password Expiration:

Passwords should expire after a maximum period of 60 calendar days (90 calendar days in case of Remote Users). A given password should not be used more than once in 180 calendar days. Additionally, the same password should not be repeated within a cycle of 6 password changes.

One Time Use of Initial Passwords:

If the administrator provides a user with an initial password, the user should change it immediately after the first time log – in to the system. (One-time password).

User Capability to Select Passwords:

Users should be provided with the capability to change their password on the login interface (after authentication).

Password Reset:

User password resets should be performed when requested by the user, after verification of identity. The new password should be a one-time password. Only the individual to whom the user- ID is assigned should request for user password reset.

Backup Passwords:

All backup passwords for critical user-IDs should be kept with the department head. The Administrator should identify the critical user-Ids and their passwords. These should be kept in individual sealed envelopes. He may be contacted in case any of the regular users are absent. These sealed envelopes should be opened only with the written permission of department head and the password should be changed immediately and replaced with the new sealed envelope. Details of such activity should be entered in the Sealed Envelope Maintenance Log Book.

Protection of Transmitted Passwords:

- Details in relation to user ID, department, password etc. should not be sent using clear text across mail systems.
- The user-ID and password should be authenticated as a w hole. Authentication failure should provide an error message to the user that does not indicate whether the user ID is correct (e.g. "incorrect login" and not "incorrect password").
- Passwords should not be included in batch logon sequences. Exceptions to this should be brought to the attention of the ITSM. The Administrator responsible for these logons should change the encoded password at least once a fortnight.

Super User Passwords:

- All the super-user passwords should be sealed in an envelope and kept in a fire proof safe. This is necessary in case the password is forgotten or the related person has left the organization without surrendering the passwords.
- These sealed envelopes should be opened with the written permission of the administrator and the password should be changed immediately and kept in a new sealed envelope.

Screen Saver Password:

Every user should use the screen saver with password, which should be activated within 5 minutes of inactivity.

Power-on Password:

- Users should be encouraged to use the power-on passwords
- Sharing of power-on passwords should not be allowed.

Password Best Practices:

Where the software permits

- Files containing passwords should be encrypted one-w ay
- Passwords should be entered in non-display fields
- Initial passwords, issued by the Systems Administrator, should be valid for two logons only.
- The software should enforce a password change following the initial logon

Disabling Default Passwords:

Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems should be promptly changed. Default passwords shipped with software should be disabled or changed.

Prohibition of Group Passwords:

Group passwords should not be allowed to the extent possible so that individual accountability is maintained. Where used, they should be maintained solely within the members of the group, and should be subject to the same controls as personal passwords. A manager or supervisor may share his or her password with a subordinate employee in the context of a group password.

Specific password policies:

Password strength or weaknesses should be analyzed for the following:

- Minimum length of password is 6.
- Password is not the same as the user's name and ID.
- Password is not equal to any user's name on the system.
- Password is alpha numeric.
- Create list of easily guessed Passwords and check if these passwords are already given.

Password Selection Rules:

Prohibition of Easy Guess Passwords
Users should be encouraged to create passwords that w ill prohibit easy guessing (i.e., passwords such as spouse's first name, Children name, etc.).

Passwords should not be based on any of the following:

- Months of the year, days of the w eek or any other aspect of the date (like date of birth, date of joining etc.)
- Family names or initials
- Vehicle registration numbers
- Employee No. / Employee Id or designations
- Project or department name or references
- Company names, identifiers or references
- Telephone numbers or similar all-numeric groups
- User ID, user name, group ID or other system identifier
- More than two consecutive identical characters
- All-number or all-alphabetic groups

Password rule enforcement procedure:

- Set up password aging via Account Policy for Window s systems and the */etc/default/passwd* file in UNIX.
- Security Administrator should obtain and run password-guessing programs to identify those users having easily guessed passwords.
- As password-cracking programs is very CPU intensive and can slow down the system on which it is running, this activity should be conducted on a standalone (not networked) system. Transfer the encrypted passwords (the dumped SAM database for Window s and the */etc/passwd* and */etc/shadow* files in UNIX) onto this standalone (not networked) system.

E-mail Security

User Responsibility:

Each employee is responsible for the contents of his / her e-mail. All e-mails must be identified with a user's name or e-mail Id to allow for individual tracking.

E-mail Attachments:

To prevent computer viruses, employees must not open attachments that are from an unknown source.

Inactivity Time Out:

If the e-mail application is not used by the user for specified number of minutes (5 as per the industry standards), the email screen at the user workstation / laptop must be inactivated. The screen must be reactivated for use, only after entering the password.

Size of Mailbox and e-mails:

The mailbox size for each user must be restricted to 5 MB. Wherever possible, the system must:

- Flash a warning message w hen a user's mailbox size reaches 4 MB.
- Lock out the user's e-mail account w hen the mailbox size exceeds 5 MB. The user must submit a formal request to the Systems Administrator for getting his account unlocked.
- Similarly, the size of incoming and outgoing e-mails must be restricted as follows:
  - 1 MB for mails received and sent outside BSNL 's network
  - 2 MB for mails sent within BSNL .

E-mail Systems as a Database:

Users must regularly move important information from e-mail message files to word processing documents, text files, databases, and other files. E-mail systems are not intended for the archival storage of important information as stored e-mail messages may be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost w hen system problems occur.

Internet mail access:

All users of e-mail should not be allowed/ authorised to send and receive mails from the Internet. The system administrator should maintain a document of the e-mail users who have the right to send and receive Internet mails.

Security of Gateway PC:

A firewall will be installed on the gateway PC that connects SSA/Circle Intranet to the Internet. This firewall will restrict all services and ports other than minimum required for e-mail applications. Current version of Anti-virus software should be loaded on gateway computer to detect and repair the viruses possibly coming through the e-mail attachments.

Monitoring of e-mail:

System administrator should periodically review the logs for the following:

- Security logs generated by the system.
- Internet e-mail received for the employees w ho are not authorised to receive internet mails
- Internet e-mail sent by the employees w ho are not authorized to send internet mails
- Virus detected and repaired

BACKUP AND RECOVERY

Information to be backed up:

- Business applications (data and program files) and operating systems residing on the servers.
- Applications (data and programs) managed by the user departments.
- Data on Workstations, desktops and laptop computers.

Responsibility:

- Systems Administrator for each server and network should be responsible for taking and maintaining backup of all data and applications as w ell as operating systems as decided by IT Department. In his absence, another personnel designated by IT Department should take the backup. This person should be given the required privileges and access to the systems for the purpose of taking backups. These privileges should be removed immediately after the System Administrator resumes his duty.
- It is the responsibility of IT users to decide on the criticality, backup and frequency of backup of the information with respect to the application systems managed by the user departments. The IT users should formally intimate the Systems Administrator about any new applications and its data to be backed up. Similarly, the Systems Administrator should be informed about discontinuing the back up of the applications systems no longer in use at the unit.
- The IT Users are also responsible for taking and maintaining the backup of all data residing on their individual workstations, desktops and laptop computers. They should take help of the Systems Administrator for taking these backups on the selected backup media.

Procedure for data backup:

- Instruction Guidelines/ procedures for taking backup of data should be developed andissued. Application backups should be taken based upon the procedures recommended by vendor and implementer for taking these backups. For other systems, should develop standard scripts and procedures, which should be issued to all concerned.
- The number of back-up sets to be maintained should be decided by System Administrator.
- It should be ensured that all the users have been logged out before taking backup.
- A list of all the data files for critical applications should be maintained by the Systems Administrator along with a brief description of the contents of those files.

Backup Media

- Instruction Guidelines for backup media should be issued detailing type of media, frequency of change in backup media and rules for rotation.
- It should be ensured that the media is regularly examined for readability of the data. The backup media should be replaced immediately after encountering the error or at predefined time intervals whichever is earlier. The backup media must be appropriately labeled and numbered, e.g. '<App>-Friday-1- 'On/Off' (where 'App' means the relevant 'application system' loan processing , payroll, mutual fund, 'Friday' denotes the day, '1' denotes the number of tapes used for the backup and 'On' or 'Off' denotes the storage of the backups).
- The data on workstations and laptops should be backed up by the respective users on the network drive or by using a portable backup device (Zip drive or other portable backup device). Network backup systems may be used for backup of all computers within the network.
- The System Administrator should track the usage of backup media and the media should be replaced after the stipulated usage.

Storage of backup:

- **On-site:**
  - On-site data back-up should be maintained in safe custody, outside the server room and in a fire-proof cabinet. The key to the cabinet should be available only with Systems Administrator and the duplicate should be kept with the location head for emergency use.
- **Off-site:**
  - Off-site data back-up should be maintained at a location identified as an 'off-site' office location for HO backup. Whenever, the backup media is moved to and from off-site location, it should be carried in sealed and tamper-proof envelope or pouch. The backup media should be stored in 'fire-proof cabinet'. The key to the cabinet should be available only with Systems Administrator. The duplicate key should be at a site different from that w here originals would be.

Backup logs:

The backup logs maintained by the System Administrator should be either manual registers or the reports generated by the system (operating systems or the applications) which should be printed and hard copies maintained. Refer to Annexure 12.4 for the format of the Backup Register.

Restoration testing:

- To verify the readability of backup media, mock restoration tests should be carried out periodically.
- It should be ensured that the restored data is deleted after successful completion of testing.

INTERNET ACCESS AND SECURITY

Use of Firewall and proxy gateway:

All Internet activity must pass through the firewall to be installed on proxy gateway server to the Internet so that access controls and related security mechanisms can be applied. All users should be authenticated with IP address, user-id and the password at the proxy gateway server. All Internet connections to and from the internal computers must be authenticated at the firewall. The router connecting the Internal network to the Internet cloud should restrict all services except minimum required for web browsing and to accomplish work.

Virus Scanning of Downloaded Internet Information:

All information downloaded e.g., email retrieval, data / ftp downloads, active-x controls, java, java applets, images etc., via the Internet must be screened with updated virus detection software prior to use.

Active Content Technologies:

- Active content (including active-x, java and javascript) must be blocked at the firewall. If need to permit them is perceived, the active content technologies must be allowed after
    I. Compensatory controls like software for detecting active content is used
    II. Proper risk assessment and business justification is evaluated
    III. Formal approval by BSNL systems administrator and business heads prior to being allowed through the firewall is taken.
    IV. Further, mitigating controls like setting the Internet browser security to ‘high’ to minimise risks must be used.

Documentation of Internet Connectivity

“Change control” plays a fundamental role in ensuring the security of the Internet connection. To accomplish proper configuration management, Internet connectivity network architecture must be completely documented and maintained, to include:
Hardware devices and components

- Firmware components
- Operating system and application software components
- Version and revision numbers of the above devices and components
- Physical and logical network addresses
- Connecting circuit numbers
- Options enabled at the software level

Logging / Reviewing:

- Routine logs of web sites visited, files downloaded, time spent on the Internet, and related information must be maintained and reviewed on a weekly basis by the Internet system administrator. He must report unusual activities to the ITSM.
- The user authentication account database must be monitored for unusual activity every week. Unusual activity includes:
  - Greater than 3 failed login attempts for a user id
  - Attempts to access root
- Utilise the tools as approved by ITSM that can highlight critical log information.
- Department heads must review reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

Monitoring of Internet Threats:

All behaviour reflecting threats to the network must be monitored. Some examples of monitored events include:

- A new server/ host attaching to the network, e.g. back orifice
- Emergence of a new machine allocated address (MAC) address on the network
- Clients response, e.g. <clients not responding> after web attends its first request.
- Well known intrusion attempts

Periodic Reconfirmation of Access Authorizations:

The Internet/Firewall system administrator must periodically reconfirm the validity of all accounts, electronic mail, and alias authorisations. The period between re-confirmations must not exceed one year. All accounts on the firewall must be approved and reported to DGM.

Internet services security levels:

Each Internet service must be evaluated for applicable security level, viz. only encryption, only authentication, encryption and authentication, and must be configured appropriately. For instance, telnet may need both authentication and encryption whereas http may only need authentication.

Access Control List (ACL):

- ACL filters (via router or multi-homed firewall) must be used to deny access to all services except those needed for business.
- ACL must be comprehensive and adequately documented describing how each entry in the ACL controls access to and from the internal network.
- ACL's must restrict all User datagram protocol (UDP) based services, except those deemed essential to the operation of the firewall system e.g., domain name server (DNS). Any services that require UDP must be evaluated and approved by Network/Communications head before implementation.

Bastion Host/ Internet servers:

- All necessary vendor security patches or upgrades must be installed on Internet servers.
- Potential targets like compilers or debuggers must not reside on the Internet servers.
- Only necessary accounts must remain active on Internet servers, e.g., system and administrator accounts.

- Root and super user accounts must not be used to connect to servers. Use a less privileged account than Super-user or change to the administrative user once connected, to enable an audit trail to indicate better who did what as super user.
- Implement operating system hardening tools to disable Super-User privileges.

File Transfer Protocol (FTP) services and Internet:

- Both inbound / outbound ftp services with Internet must not be allowed, unless approved by Head-IT.
- When approved, the following guidelines must apply to ftp services:
  - The system administrator for the Internet servers must ensure that anonymous file transfer (Anon FTP) systems are disabled.
  - All FTP sessions must be authenticated, encrypted and must be logged.
  - The FTP root directory must not be at the system root level and the directory used must be “chrooted” if supported by the operating system.
  - FTP sessions must be configured to disconnect after acceptable period of inactivity.
  - Unsuccessful login attempts must also be disabled or disconnected. Audit trail for all unsuccessful login attempts must be available.
  - Outbound FTP must be allowed only via proxy accounts on the firewall.

Internet mail:

- All Internet mail must be provided through an approved mail server of BSNL .
- All mail services must be provided through the firewall.
- SMTP traffic must be handled by a dedicated SMTP proxy (e.g., SMAP/SMAPD), and not allowed to pass through the firewall to an internal mail server. Dangerous SMTP traffic (e.g., pipe symbols) should be rejected and logged by the proxy.
- Internal host name and addresses should be hidden from mail headers. For outgoing mail messages outbound email headers must be selectively rewritten so that all email appears as if it originated from the firewall or external SMTP relay.
- SMTP message size must be appropriately restricted to the capabilities of the mail servers.
- The following configuration practices must be applied for sendmail on mail servers:
  - Insecure sendmail configuration options such as WIZ, VRFY, EXPN and DEBUG must be disabled.
  - The sendmail.cf file must allow only a minimal list of "trusted users”.
  - The sendmail aliases file must be configured securely with minimum permissions.
  - The sendmail mail queue file and mail configuration file must be configured securely, with only the minimum permissions necessary for operation.”

WEB SERVER SECURITY

A Web server typically stores information intended for widespread publication. It may also store information requiring restricted access such

- Server log files
- System software and configuration files
- Applications software and configuration files
- Password files
- web server is vulnerable to attacks such as:
- Defacement
- Known worms like Code Red and Nimda as well as unknown worms
- Buffer overruns
- Hidden field manipulation

Using the access controls provided by both the server operating system and by the Web server software, we can reduce the likelihood of inadvertent information disclosure or corruption, and violations of confidentiality and integrity. In addition, using access controls to limit resource use can reduce the impact of a DoS attack, a violation of availability.

Protection for Web server components:

Identify the protection needed for files, devices, and objects specific to the Web server.
In addition, determine if our Web server's operating system provides the capability to limit files accessed by the Web services' processes. These processes should have read-only access to those files necessary to perform the service and should have no access to other files (such as server log files). If this capability is not available, skip some of the following steps. In this event, we need to implement other security controls (described below) to limit the exposure. Use Web server host operating system access controls to enforce the following:

- Public Web content files can be read but not written by Web service processes.
- Web service processes cannot write the directories where public Web content is stored.
- Only processes authorized for Web server administration can write public Web content files.
- Service processes can write web server log files but log files cannot be read or served as Web content. Only administration processes can read web server log files.
- Any temporary files created by Web service processes (such as those that might be generated in the creation of dynamic Web pages) are restricted to a specified and appropriately protected subdirectory.
- Access to any temporary files created by Web service processes is limited to the service processes that created these files.

Measures against DoS attacks:

Limit the use of resources by the Web server host operating system to mitigate the effects of Denial of Service (DoS) attacks.
Resource-intensive DoS attacks against a Web server host operating system include:

- Filling file systems with extraneous and incorrect information. Some systems will not function if specific resources (such as file systems) are unavailable.
- Filling primary memory with unnecessary processes to slow down the system and limit Web service availability

Logging information generated by the Web server host operating system may help in recognizing such attacks.
Provide the following controls to mitigate the effects of such attacks:

- Separate directories for log files and other information from system directories and user information. You can establish effective boundaries between these information objects by specifying separate partitions and/or disk locations
- Assigning priorities to Web service processes can help to ensure that high priority processes obtain sufficient resources, even while under attack.

These controls will not fully protect our Web server against DoS attacks. However, by reducing the impact of these attacks, the Web server may be able to "survive" during the time period when the DoS attacks are occurring.

Time-outs configuration:

Configure time-outs and other controls to mitigate the effects of DoS attacks. Another type of DoS attack takes advantage of the number of simultaneous network connections by quickly establishing connections up to the maximum permitted such that no new, legitimate users can gain access. Network connection time-outs (time after which an inactive connection is dropped) should be set to a minimum acceptable time setting. Established connections will then timeout as quickly as possible, opening up new connections to legitimate users. This only mitigates the

effects; it does not defeat the attack. If the maximum number of open connections (or connections that are halfopen, i.e., the first part of the TCP handshake was successful) is set to a low number, an attacker can easily consume the available connections with bogus requests. By setting the maximum to a much higher number, the impact of such attacks may be reduced, but additional resources will be consumed.
As above, it is worth noting that these controls will not fully protect the Web server against DoS attacks. However, by reducing the impact of these attacks, the Web server may be able to "survive" during the time period when the DoS attacks are occurring.

Web Server configuration to restrict content distribution:

Configure the public Web server so it cannot serve files that are outside of the specified file directory tree for public Web content. This may be a configuration choice in the server software or it may be a choice in how the server process is controlled by the operating system. Ensure that such files (outside of the specified directory tree) cannot be served, even if users know the names (URLs) of those files. Avoid the use of links or aliases in public Web content file directory tree that point to files elsewhere on server host or network file system. If possible, disable the ability for Web server software to follow links and aliases. As stated earlier, Web server log files and configuration files should reside outside of the specified file directory tree for public Web content.

Configure Web server software access controls:

Perform the following steps:

- Define a single directory and establish related sub-directories exclusively for Web server content files, including graphics but excluding CGI scripts and other programs.
- Define a single directory exclusively for all external programs executed as part of Web server content.
- Disable the execution of CGI scripts that are not exclusively under the control of administrative accounts. This is accomplished by creating and controlling access to a separate directory intended to contain authorized CGI scripts.
- Disable the use of hard or symbolic links as ordinary files and directories.
- Define a complete Web content access matrix. Identify which pages are restricted and which pages are accessible (and by whom).

Most Web server software vendors provide directives or commands that allow system administrator to restrict user access to public Web server content files.
For example, the Apache Web server software provides a Limit directive, which allows restriction as to which optional access features (such as New, Delete, Connect, Head, and Get) are associated with each Web content file.
The Apache Require directive allows option to restrict available content to authenticated users or groups.
Many of the directives or commands can be overridden on a per directory basis. The convenience of being able to make local exceptions to global policy is offset by the threat of a security hole being introduced in a distant subdirectory—which could be controlled by a hostile user. We should disable a subdirectory's ability to override top-level security directives unless that override is required.

Disable the serving of Web server file directory listings:

The Web protocol (HTTP) specifies that a URL ending in a slash character is treated as a request for a listing of the files in the directory with that name. As a general rule, we should prohibit our server from responding to such requests, even if the general public can read all of the files in the directory. Such requests may indicate an attempt to locate information by means other than that intended by our Web site. Users may attempt this if they are having difficulty navigating through our site or if a link appears to be broken. Intruders may attempt this to locate

information hidden by our Web site's interface. We may want to investigate requests of this type found in our server log files.

FIREWALL SECURITY

Use of Firewall and proxy gateway:

All Internet activity must pass through Firewall to be installed on Proxy gateway server to the Internet so that access controls and related security mechanisms can be applied. All users should be authenticated with IP address, user-id and the password at the proxy gateway server. All Internet connections to and from the internal computers must be authenticated at the firewall. The router connecting the internal network to the Internet should restrict all services except minimum required for web browsing and to accomplish work.

Remote Firewall Administration:

- Any remote access over untrusted networks to the firewall for administration must use strong authentication, such as one-time passwords and/or hardware tokens.
- Firewall administration should be directly from the attached terminal. Physical access to the firewall terminal should be limited to the firewall administrator.
- Where remote access for firewall administration must be allowed, it should be limited to access from other hosts on BSNL's internal network. Such internal remote access requires the use of strong authentication, such as one-time passwords and/or hardware tokens.
- All firewall administration must be performed from the local terminal - no access to the firewall operating software is permitted via remote access.

Virtual Private Networks (VPN):

Any connection between firewalls and Internet shall use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network. All VPN connections must be approved and managed by the Network & Communication Security Administrator. Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.

Domain Name Server (DNS):

It is strongly recommended to have separate DNS, web server and email server .If the firewall is running as a DNS server, then the firewall must be configured to hide information about the network so that internal host data are not advertised to the outside world.

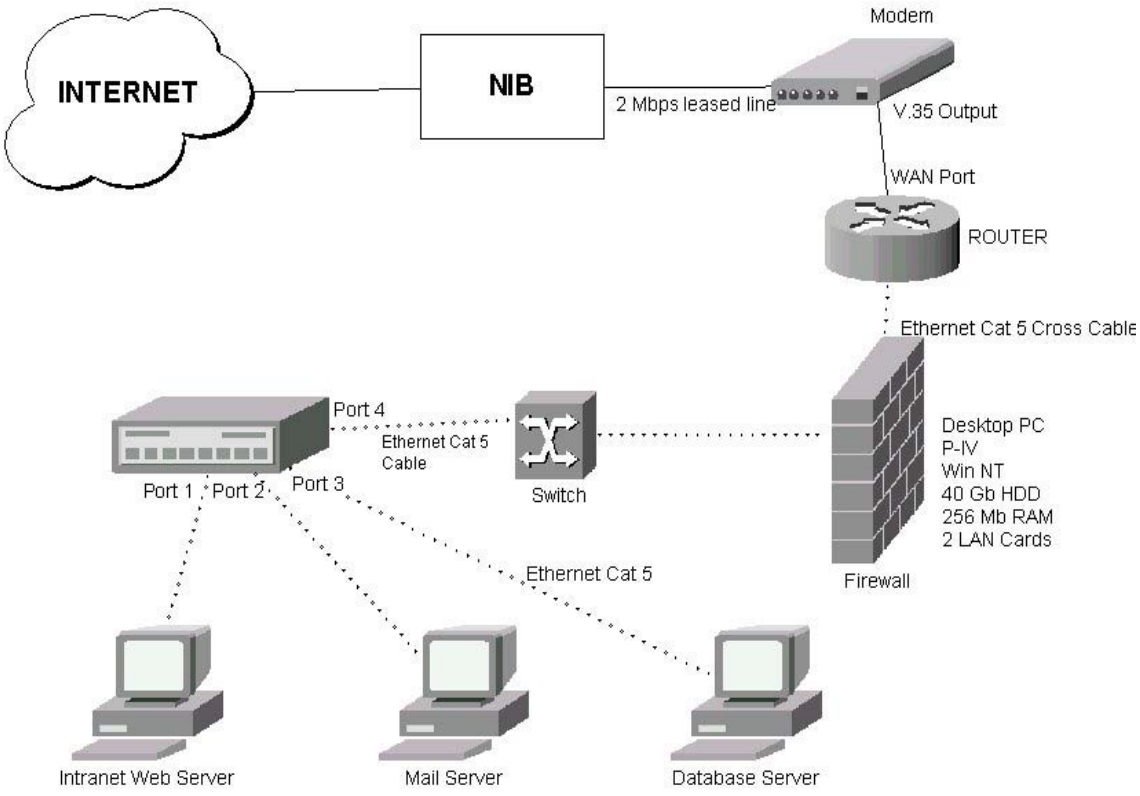
Firewall Backup:

To support recovery after failure or natural disaster, backup of data files as well as system configuration files must be done. The firewall (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Another backup alternative would be to have another firewall configured as one already deployed and kept safely so that in case there is a failure of the current one, this backup firewall would simply be turned on and used as the firewall while the previous one is undergoing a repair. At least one firewall shall be configured and reserved (not-in-use) so that in case of a firewall failure, this backup firewall can be switched in to protect the network.
Some of the Routers already have Security Features built into it (eg. CISCO PIX). For such networks, where Routers have been used, a separate FIREWALL need not be procured. Other

networks, which have been set up using Switches and Converters, a separate FIREWALL will have to be procured.

Following are some of the features which should be available in the FIREWALL:

1. It should be scalable from a min. of 25 users to at least 100 users.
2. Should have a high MTBF and it should be able possible to pair it with another similar appliance to configure it for failover working.
3. It should be possible to dynamically update the firewall with the latest patches and updates.
4. Multiple levels of user authentication should be possible.
5. Should support URL filtering based on type of content, time of day etc.
6. Remote management of the Firewall should be possible.
7. Should have capability to support VPN.
8. It should be possible to log reports based on various user-defined parameters like host to host connections, Internet activity, individual activities etc.
9. The Security Policies, as defined by the user should be implemented in the Firewall.
10. The Firewall should support both Dynamic Stateful Packet Filtering and Security Proxying.
11. Packet Filter throughput should be better than 100 Mbps.
12. Static and Dynamic NAT should be possible.
13. Spoof Detection should be possible.
14. Port / Site blocking should be possible.



FIREWALL INPLEMENTATION IN INTRANET

Procedures for Server Room:

User Accounts:

Firewall should not be used as general-purpose server. The only user accounts on the firewall should be those of the Network and Communication Security Administrator and backup administrator. In addition, only these administrators should have privileges for updating system executables or other system software. Only the Network and Communication Security Administrator and backup administrator will be given user accounts on the firewall. The Network and Communication Security Administrator or Firewall backup administrator must do any modification of the firewall system software.

Network Trust Relationships:

Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures. All connections to approved external networks should pass through BSNL firewall.

Documentation:
The operational procedures for the Firewall and its configurable parameters should be documented, updated, and kept in a safe and secure place. This ensures that if the Network and Communication Security Administrator resigns or is otherwise unavailable, the backup administrator can read the documentation and rapidly pick up the administration of the firewall. In the event of a break-in such documentation also supports trying to recreate the events that caused the security incident.

Physical Firewall Security:

Physical access to the firewall must be tightly controlled to preclude any unauthorised changes to the firewall configuration or operational status, and to eliminate any potential for monitoring firewall activity. In addition, precautions should be taken to ensure that proper environment alarms and backup systems are available to assure the firewall remains online. Firewall should be located in a controlled environment, with access limited to the Network and Communication Security Administrator and the backup firewall administrator.

Upgrading the firewall:

The firewall software and hardware components should be upgraded with the necessary modules to assure optimal firewall performance. The firewall administrator should be aware of any hardware and software bugs, as well as firewall software upgrades that may be issued by the vendor. If an upgrade of any sort is necessary, certain precautions must be taken to continue to maintain a high level of operational security. To optimize the performance of the firewall, all vendor recommendations for processor and memory capacities shall be followed. Hardware and software components shall be obtained from a list of vendor-recommended sources. Any firewall specific upgrades shall be obtained from the vendor. Virus checked CDROM or ftp to a vendor's site should be used for upgrades.

Logs and Audit Trails (Audit/Event Reporting and Summaries):

Firewall capabilities for logging traffic and network events should be enabled. Firewall audit trail logs should cover hardware and disk media errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound e-mail traffic, TCP network connect attempts and in-bound and out-bound proxy traffic type.

Network Security Coordinator- Roles and Responsibilities related to Firewall Administration:

The firewall's system integrity database shall be updated each time the firewall configuration is modified. System integrity files must be stored on CD-ROM or off-line storage. System integrity shall be checked on a regular basis on the firewall in order for the Network and Communication Security Administrator to generate a listing of all files that may have been modified, replaced, or deleted.
The firewall administrator must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.
Periodic Upgrading of the firewall, firewall backup, Incident handling and restoration procedures should be carried out.

VIRUS PROTECTION

What is a 'Computer Virus'?
A computer virus is an unauthorized and malicious program, which replicates itself and spreads onto various data storage media such as floppy diskette, magnetic disk, tapes and across the network. The viruses are designed to spread from one file to another, from one program to another, from one machine to another, and even from one network to another. Viruses threaten the integrity and availability of data. The symptoms of virus infection include considerably slower response time from the system, inexplicable loss of data, erroneous change in file dates, increase or decrease in file size or total failure of computer system. No effort shall be spared and necessary time; resources and money will be invested to protect the IT resources against the harmful and destructive intrusion of computer viruses.

Updates of Virus 'DAT files':

These are the files, which contain the data on virus signatures. Virus Helpdesk should maintain these 'DAT files'. The user should download the data from the Internet website of the company the anti-virus software is from. The Administrator should also copy these DAT files on all the servers.

Updating of 'DAT files' on client computers/ network nodes

Once the updates of virus DAT files are copied on the central host computers (servers), an operating system job should be scheduled in the network server for pushing these DAT file updates onto client computers/ network nodes connected.

Updating of 'DAT files' on remote locations

Virus can enter the network through an infected file sent from some other locations. There should be provision made to update virus definitions at remote locations also.

Anti-Virus software upgrades
The upgrades are the newer versions of the anti-virus software. newer versions/ engines of Anti-virus programs should be procured and provided in regular and timely manner.

Virus protection - some specific procedures:

- It should be ensured that the Anti-virus software is installed and active on every machine. Password protection should be there so that the users do not disable the Anti-virus check.

- The Anti-virus software should be run at least once in a day by each user and it should be properly scheduled.
- Every diskette, DAT and DLT tape should be scanned for virus before use.
- Systems should be implemented to review the anti-virus software activity/ logs, especially to check whether the IT users are running the Anti-virus system regularly on their desktop computers.
- Upon encountering the virus problem, the Anti-Virus software should stop the computer operations, delete the related files and clean the affected areas. The other options such as 'continue' and 'move to a directory' in Anti-Virus check should not be enabled.
- Messaging and Anti-virus: The Anti-Virus software for messaging system (e-mail) should be implemented. If the virus is found in mail attachment file, this file should be deleted and the sender should be informed. The recipient would get the remaining message.
- Checking the software downloaded from Internet: Software/ data downloaded from outside sources such as Internet may contain a virus. Before such software is decompressed, the users should always have 'Auto-Protect' active on such workstation. In order to provide more security, he should log out of all files servers and terminate all other network connections. Before executing the software, it should be screened with the approved Anti-virus package. If a virus is detected, the Security Administrator should be notified immediately and no further work should be carried on the affected machine until the virus has been shown to be eradicated.