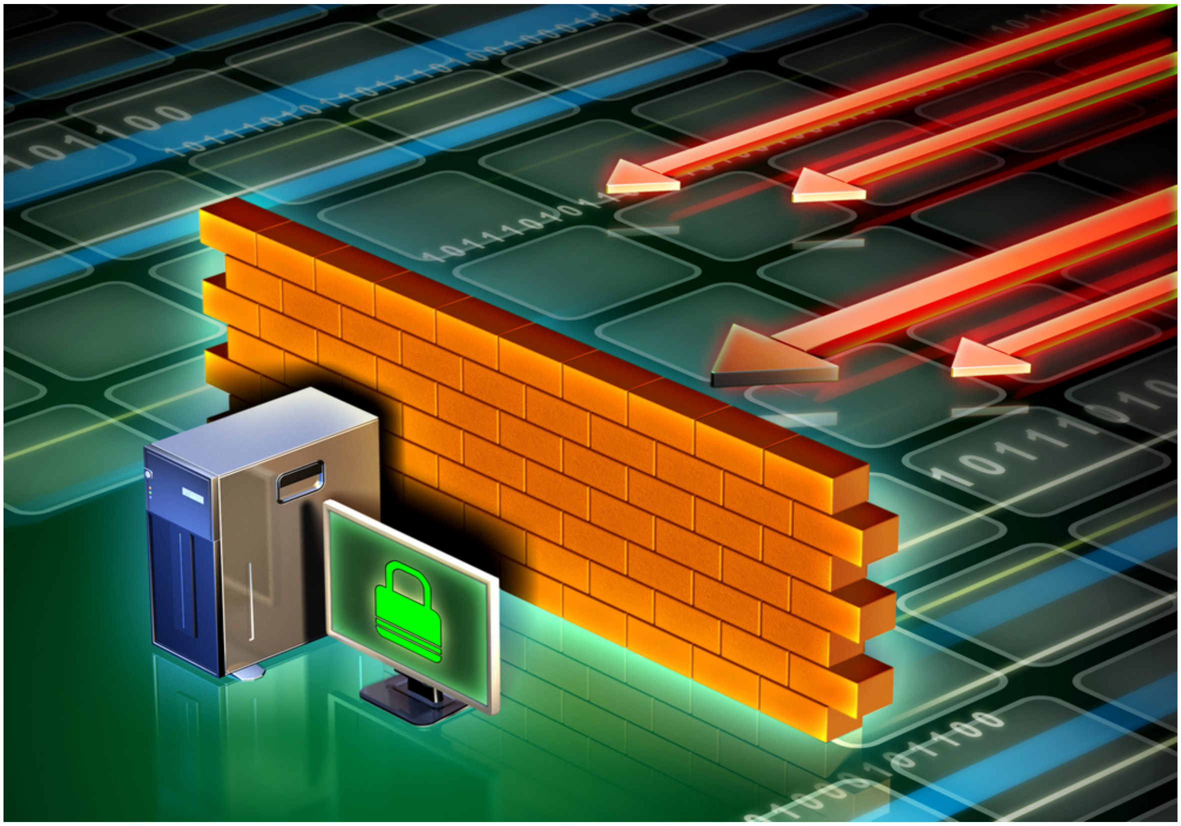
FIREWALL
AUDIT
CHECKLIST



G. M. Faruk Ahmed

CISSP, CISA, CDCP, CEH

www.gmfaruk.com

FIREWALL CHECKLIST

Pre Audit Checklist

1. Obtain previous workpapers/audit reports.

2. Obtain the Internet Policy, Standards, and Procedures relevant to the firewall review.

3. Obtain current network diagrams and identify firewall topologies.

4. Identify the type and version of firewalls implemented.

5. Identify objectives of firewall installation.

6. Identify the operating system supporting the firewall.

7. Identify all Internet Service Providers (ISP) and Virtual Private Networks (VPN).

8. Obtain an understanding of the ISP and VPN contracts.

9. Identify whether methods other than the Firewall are used to provide access to the Internet (from trusted networks) and from the Internet (from untrusted networks) is permitted (i.e., modem, dial-in, etc.).

10. Obtain vendor Firewall default configuration, documentation and update availability.

Administration Review

11. Is there documentation that clearly defines the roles and responsibilities of firewall administration, including training and testing of firewall configuration?

12. Is there a list of authorized firewall administrators? (Identify primary and backup administrators).

13. Has the effectiveness of backup administrators in support of the firewall been tested?

14. Is there someone who is responsible for keeping up with current security advisories?

Access Control

15. Is there a process used to authorize employees and non-employees access (add, change, delete) to the Internet?

16. What levels of access are privileges granted?

17. Assess the timeliness and completeness of the methods used.

18. Is there a password policy?

19. Have password control features been implemented for all accounts? (I.e. required use, minimum length, periodic changes, etc.).

20. Have the default accounts either been disabled or the original password changed from the vendor provided values.

21. Are there controls that ensure that access to the Internet is granted to only those authorized individuals?

22. Obtain a list of users with access to the firewall and reconcile to documented approved requests.
    Is each user uniquely identifiable?

23. Evaluate whether the authentication methodologies (i.e., proxy) used are effective.

24. Is non-employee access appropriate?

25. Does the security administrator periodically review the users that have access to the Internet?
    When was the most recent review?

26. Are there periodic reviews of inactive accounts?
    What are the actions taken to resolve the discrepancies?

27. What are the security controls used by the VPN in securing access to xyz trusted networks?

28. Are there security controls over the use of modems and other methods (i.e. dial-in) used to access xyz's trusted networks?

29. How is public access to the Web Servers protected by the firewall?

Firewall Configuration

30. Evaluate the appropriateness of Firewall topologies implemented.

31. What is the current hardware and software configuration of the Firewall?

32. Have all updates identified by the vendor been applied.

33. Is there a DMZ?
    Does the firewall properly separate the DMZ from the inside network and the outside network?

34. Is there is a single point at which the internal network can be separated from the Internet?

35. Review Firewall documentation to gain an understanding of the Firewall's capabilities and limitations.

36. Is there a Firewall filter change control procedure?

37. Identify the rules that should be enforced by the firewall (what services are allowed between source and destination).

38. Is encryption used for authorized services?

39. What are the firewall rules currently in place?

40. What are the filtering techniques used to permit or deny services to specified host systems?

41. Is Network Address Translation being performed and, if so, is it properly configured?

42. Evaluate the order of firewall rules for effectiveness.

43. Does the firewall have the following controls in place?
    URL screening.
    Port blocking.
    IP spoofing.
    Packet screening.
    Prevent Denial of Service attacks.
    Incoming Java or ActiveX screening.
    Anti-virus protection.

44. Does the firewall support a "deny all services except those specifically permitted" policy.

45. Is the Firewall configured according to xyz Standards and Guidelines and does the firewall effectively enforce the Internet security policy?

46. Is the effectiveness of the firewall in enforcing the security policy reported to management?

Monitoring

47. Is there an Intrusion Detection System (IDS) in place?

48. What are the threats for which response has been automated (e.g. denial of service attacks, spoofing)?

49. If IDS has not been implemented, determine the extent of intrusion detection automation.

50. Are the firewall activities logged?
    Are there procedures in place to monitor and act upon any inappropriate activities?

51. Are the actions of staff who have privileged access to the firewall authenticated, monitored and reviewed?

52. Is logging and reporting procedures in place to monitor and act upon any inappropriate activities?

53. Are all inbound services, outbound services, and access attempts to or through the firewall that violates the policy are all logged and monitored.

54. How frequently monitoring is performed?

55. Have alarms been set for significant events or activities?

56. What tools are used to help trend analysis?

57. Do the logs contain sufficient data for user accountability, type of transaction, date/time stamp, terminal location, etc?
    Are the logs protected to prevent modifications?
    How long are the logs kept?
    What media are the logs stored on?

58. What process is used to report, follow-up, evaluate, and resolve all incidents?

59. Obtain copies of firewall reports for review.

60. Are the firewall reports adequate in providing administrative staff with necessary information to help analyze firewall activities (attacks, defenses, configurations and user activities)?

61. What are the processes used to follow-up and resolve incidents?

62. Is the firewall periodically tested from xyz's trusted and untrusted networks.

63. What is the effectiveness of the firewall in enforcing xyz's security policy as reported to management?

Physical Security

64. Are there physical methods to prevent unauthorized personnel from accessing Firewall systems?

65. Is there a list of authorized personnel permitted access to Firewall computer rooms?

66. Do all of the authorized personnel need access?

67. Are there physical methods to prevent unauthorized personnel from accessing consoles, closets, routers, etc?

Firewall Change Controls

68. Is there a firewall change control procedure in place?
    Is there documentation for all firewall changes?
    Have all of the changes been authorized?

69. Are there procedures to inform firewall administrator of any new security-related problems or patches are available arid are applied adequately and timely.

Backup and Recovery

70. Is there a Disaster recovery contingency plan?
    Has the recovery been tested?

71. Evaluate the adequacy of backup and recovery procedures (including retention).

72. How frequently are backups performed?

73. Is encryption used when performing backups?

74. What were the results of the last successful backup test?

Operating System

75. Verify the operating system type and version, including patch history.

76. Evaluate account management process.

77. Assess the adequacy of the approval process.

78. Identify types of accounts authorized to have access.

79. Evaluate the adequacy of access controls and authentication.

80. Assess appropriateness of all accounts.

81. Assess the adequacy of password controls.

82. Do all of the network services need to be in place?

83. Identify & evaluate the effectiveness of performance monitoring and control procedure.