Network Architecture Review Checklist

Version 1.0

www.garage4hackers.com

Sr. No.	Review Area	Question/Control description	Suggested Verification step	Evidence/Artificats
1	Documentation	Has the design of the network been formally documented?	1)Check if a documented network diagram exists? 2)Check that the design has been through a formal review and sign-off process and that it is now under change control.	1)Network Diagram 2)Version Control 3)Formal review & sign-off
2	Documentation	Have the security requirements of the organization been identified and incorporated in the design?	1)Determine if the requirements for the network have been formally documented. 2)Confirm that security requirements are addressed (eg confidentiality of network traffic,encryption) 3)Check if sizing and growth information have been incorporated in the design.	1)Network Design document 2)Network Capacity Planning document
3	Firewall rule Change Management	Is the implementation and change of traffic filtering rule sets subject to strict change management procedures?	1)Verify the firewall rules & respective approved change management requests/tickets 2)Ensure all changes are formally documented and include at minimum the date of the change, the name of person making the change and the reason.	1)Change management requests/tickets 2)Firewall change management procedure.
4	Firewall rule Review	Periodic review of Firewall rules	1)Check if periodic review of firewall rules is carried out? 2)Check if not used/expired firewall rules are removed/disabled?	1)Firewall rule review 2)Firewall rules
5	Intrusion Detection/Prevention	Are Intrusion detection system sensors placed in the correct location to detect attempts to penetrate the network?	1)Check if IDS/IPS sensors are placed in a position to detect attempts to penetrate.(eg before or after firewalls or all points of entry and exit in a network). 2) Check if the critical & sensitive systems are protected by IDS/IPS	1)Network Diagram 2)Discussion with Network Admin/Architect
6	Network Addressing	Does network addressing scheme that is specified in the design make the network scalable,optimal & manageable?	1) Are the network address ranges contiguous and facilitate a hierarchical approach to network? 2)Is the private address ranges being used facilitate easy diagnosis of network problems. 3)Does it make the networks more difficult to extend?	1) Network Addressing Scheme 2)Router/Switch configuration 3)Discussion with Network Admin/Architect
7	Network Design	Does the design of the network incorporate coherent standards/Regulations?	1)Check if the design of the network complies with relevant & applicable standards & regulations (e,g RBI guidelines,PCI-DSS,Data Privacy)	1) Verify compliance against relevant applicable standards

8	Network Design	Is consistent naming standards included in the design	1)Check if the design incorporates consistent naming standard for the various components in the network.	1) Veify for naming standards in the design document
9	Network Filtering	Are network filtering devices configured to filter specific types of traffic (eg IP address, port), block or restrict particular types or sources of traffic, and limit the use of communications that are prone to abuse?	1) Check firewall rules are configured with default-deny stance 2) Check firewall rules for traffic filtering ports by IP address & ports and not ANY ANY.	1)Firewall rules
10	Network Routing	Are the routing methods used in the design making the network vulnerable to errors or latency?	1)Are both static and dynamic routing being used? 2)Review the routing table and verify that the route followed is optimal for dynamic routing?	1)Router configuration 2)Routing table
11	Network Segregation	Does the design of the network include distinct sub-networks, protected by rule based traffic filtering?	1) Check if network is divided into sub-networks based on criticality 2) Check if the traffic between the sub-networks are protected by a network filtering device (e,g firewall,core switch with FWSM).	1) Network diagram 2) Firewall rules/ACL's
12	Network Segregation	Does the network make use of VLAN's?	1) Confirm if VLAN's are being used and check if networks are segregated based on criticality.	1)Network Diagram 2)VLAN configuration 3)Core Switch configuration
13	Network Segregation	Is Inter VLAN routing enabled?	1) Check if inter VLAN routing is enabled? 2) Review the Core Switch ACL's	1) Switch Configuration 2)VLAN config details
14	Network Segregation	Verify if appropriate segregation is implemented between wired and wireless networks?	1) Check if the wired & wireless networks are segregated by a firewall.	1)Network Diagram 2)Discussion with Network Admin/Architect
15	Network Segregation	Public facing devices placed in DMZ	1) Are all public facing devices placed in DMZ 2)Are all public facing systems placed on different DMZ's based on criticality & functionality of the system.	1)Network Diagram 2)Discussion with Network Admin/Architect
16	Perimeter Security	Have all entry/exit network points are clearly identified in the network design.	1)Confirm that all entry / exit points are clearly identified in the network design. 2)Check that all entry / exit points serve a key business purpose. 3) Verify the security requirements for all entry/exit points	1)Network diagram 2)Discuss with the network admin the purose of each entry/exit points 3)Encryption,VPN,access control filtering for each entry/exit point
17	Perimeter Security	Have mechanisms been implemented to control all traffic that enters and leaves the network (eg through the use of firewalls/UTM or screening routers)?	1)Check if all entry & exit points are protected by appropriate filtering using firewalls,UTM or screening routers?	1)Network diagram 2)Firewall config 3)Discussion with Network Admin/Architect

18	Third Party Connections	Third party connections to the network been identified & secured	1) Have all third party connections identified? 2)Ascertain if access is restricted to only certain parts of the network. 3) Verify if appropriate level of encryption is implemented (i.e VPN)	1)Network diagram 2)Firewall config 3)Discussion with Network Admin/Architect
19	Remote User Access	Remote user access protection	1)Request an explanation of how remote users are authenticated. 2)Check that all remote connections are logged. 3)Confirm that remote access logs are reviewed. 4)Confirm user access review is carried out regularly	1)VPN configuration 2)ACS/RSA configuration 3)Discussion with Network Admin
20	Unauthorized connections	Regular audit of unauthorized connections	1)Establish if a variety of methods are employed to detect unauthorised connections (eg manual audit, review of telecommunications supplier bills, use of network discovery tools, war-dialling). 2)Determine how often checks are carried out. 3)Check that when external connections are no longer required, they are removed promptly. 4) Regular Wardriving exercises are carried out to locate rogue access points.	1)Network Security Policy 2)Discussion with Network Admin & Information Security Team
21	Authentication Authorization & Accounting	AAA systems are in place for network devices	1) Check TACACS or RADIUS is in place for network and security devices	1)TACACS/RADIUS/ACS configuration
22	Network Logging	Ensure appropriate logging and review is carried out	1) Ensure all devices events are logged and directed to syslog 2)Verify if log access review is carried out 3) Check the availability of Log correlation tools and effective use of it.	1) Discussion with Network Security Team 2) Check the adherence for Policy interms of logging
23	Time Server	All network & security devices are time synchronized	1) Check the availability of NTP server 2) Check if all devices get their time synchronized from this NTP server	1) NTP server configuration

24	Network Resilience	To ensure that the network is suppported by a robust & reliable set of hardware & software	1) Have all single point of failures (SPOF) in the network identified? 2)Request information on redundancy measures that have been employed(eg multiple carriers, dual operations centres). 3)Confirm that all critical network devices can be reached via more than one path. 4)Check that network protocols have been implemented that are capable of re-routing traffic in the event of network failure (eg OSPF). 5)Check that resilience arrangements for communication links do not ultimately depend upon common circuits (eg from a common carrier). 6)Check that arrangements to use alternative service providers are adequate (eg by reviewing contractual documentation that exists).	1) BCP/DR documents for Networks 2) Susceptability Analysis reports 3)Network diagram 4)Discussion with Network Admin
25	Network Resilience	Network resilience arrangements are tested.	1)Ensure that the fall-back measures specified exist and have been tested to ensure they work correctly. 2)Is there a programme of testing to ensure fall-back mechanisms operate correctly. This testing should simulate, as far as possible, the live operational conditions that will be required (eg similar volumes of traffic).	1)BCP/DR test reports
26	Network Resilience	Preventive maintenance is carried out	1)Is preventive maintenance conducted on a regular basis? 2)Are proper records being kept of the equipment type, make, model and its service history?	1) Preventive maintenance reports 2) Network asset register 3) Capacity planning documents

Disclaimer

All part of this document may be reproduced,stored in a retireval system,or transmitted in any form or by any means, electronic, mechanical ,photocopying ,recording, scanning or otherwise.While the author & G4H have used their best efforts in preparing this work,they make no representation or warranties with respect to the accuracy or completeness of the content of this book.The advice and controls herein may not be usable for your situation, you should cosult a professional where appropriate.Neither G4H or the author shall be liable for any loss of profit or any other commercial damages,including,but not limited to,special,incidental,consequential or other damages.