

UNCLASSIFIED

Gateway Certification Guide V3.4.1



Australian Government
Department of Defence

Defence Signals Directorate

GATEWAY CERTIFICATION GUIDE

VERSION 3.4.1

Point of Contact: Advice and Assistance Team

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

© Commonwealth of Australia 2005

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the *Copyright Act 1968*, all other rights are reserved.

UNCLASSIFIED

UNCLASSIFIED

Document Change Record

Version	Changed By	Date	Changes
3.4	Advice and Assistance	July 05	Policy and consistency check.
3.4.1	Advice and Assistance	October 05	Update for September 2005 ACSI 33 and PSM 2005.

UNCLASSIFIED

Table of Contents

Introduction 4
Gateway Certification Process 5
1.0 Gateway Risk Assessment 8
2.0 Gateway Policy Development Process 9
 2.1 Access Policy 9
 2.2 Security Policy 9
 2.3 Contingency Policy 11
 2.4 Incident Detection and Response Policy 11
3.0 Gateway Design Methodology 14
 3.1 Gateway Major Components 14
 3.2 Mandatory Security Design Criteria 16
 3.3 Risk Based Security Design Criteria 18
 3.4 Critical Security Configuration 20
 3.5 Design Documentation 20
4.0 Gateway Security Management 22
 4.1 Security Administration Tasks 22
 4.2 Proactive Security Checking Tasks 24
 4.3 Proactive Security Audit Checks 25
 4.4 Contingency Plan 26
 4.5 Incident Detection and Response Plan and Procedure 26

UNCLASSIFIED

Introduction

1. Australian Government agencies are required by the Protective Security Manual (PSM) to consider the security of their electronic information systems and to implement safeguards designed to adequately protect these systems. The degree of protection for these systems must be commensurate with the risk.
2. The Information Security Group of the Defence Signals Directorate (DSD) has identified a continuing need for security perimeter (or gateway) protection. This protection is essential when an organisation connects to an untrusted network. The number of threats to systems, data and applications, and the high level of threat likelihood dictates that appropriately managed safeguards are required to protect organisation information systems so as to minimise the risk of intrusion to or compromise of these systems.

Purpose

3. The Gateway Certification process aims to provide agencies, or a Service Provider to Australian Government with an independent assessment that their gateway has been configured and managed to Australian Government standards, and that appropriate safeguards are implemented and operate effectively.¹ This assurance provides clients using the gateway services with a reasonable level of trust in the service provided. This document is designed to assist agencies seeking or renewing certification.
4. This document serves as a reference detailing the areas of specific concern to the assessors conducting the certification and allows organisations to scope, cost and resource the security requirements in advance of the certification process itself. Accordingly, this document provides a reference for verification of any gateway.
5. This document should be used in conjunction with the Australian Government Information and Communications Technology Security Manual, also known as ACSI 33, produced by DSD. Where certification by DSD or an I-RAP assessor is intended, the Gateway Certification Checklist, found with this guide on the DSD website (<http://www.dsd.gov.au>), is used and can also assist in preparation for certification.

Related Documentation

Agencies and I-RAP assessors are strongly encouraged to seek further guidance from the following documents:

- The Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2005.
- The Gateway Certification Checklist, V2.2.1.
- Protective Security Manual (PSM), 2005.

¹ The Infosec Registered Assessors Program (I-RAP) is a DSD initiative designed to register suitably qualified information security assessors to conduct work to Australian Government standards. A Gateway Certification performed by an I-RAP assessor for gateways classified up to PROTECTED or RESTRICTED is recognised by DSD.

UNCLASSIFIED

Keywords

The table below defines the keywords used within this document to indicate the compulsory requirements for DSD or I-RAP certification.

Keyword	Interpretation
MUST	The item is mandatory for certification.
MUST NOT	Non-use is mandatory for certification.
SHOULD	Valid reasons to deviate from the requirement may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by the certifying authority during the certification process. Note: Agencies deviating from a SHOULD , MUST document the reason(s) for doing so.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by the certifying authority during the certification process. Note: Agencies deviating from a SHOULD NOT , MUST document the reason(s) for doing so.
RECOMMENDS RECOMMENDED	A recommendation or suggestion. Note: Agencies deviating from a RECOMMENDS or RECOMMENDED , are encouraged to document the reason(s) for doing so.

Definitions

6. **Organisation**, or any of its derivations, is used to refer to any Government Agency or Government Department as well as any Service Provider seeking to provide services to Australian Government.

7. Please refer to the glossary in ACSI 33 for a comprehensive list of definitions used within this document.

Gateway Certification Process

8. Gateway Certification is a process to verify that a gateway is being managed to Australian Government standards. This certification process does not provide any guarantee that the gateway will not be compromised rather that its design, management and operation is appropriate to the assessed level of risk. Checks will provide a degree of assurance that management processes are satisfactory for the continued, secure operation of the gateway.

9. The certification process can be broken down into five distinct phases. As per Part 2, Chapter 7 of ACSI 33 for more details.

UNCLASSIFIED

Conditions of Certification

10. For further information on conditions of certification please refer to ACSI 33 Part 2, Chapter 7.

11. DSD can provide, on a cost recoverable basis, certification for gateway environments.

12. As part of the certification letter, DSD will advise the specific conditions of certification. Failure to meet these conditions may result in DSD withdrawing the certification. The broad conditions include but are not limited to:

- Advice to DSD on major changes to key components, including policy, before these changes are implemented.
- Discussion with DSD on any changes to the analysed threat level.

13. The different levels of certification are:

- Full Certification: This is awarded to gateways that are compliant with the requirements for gateway certification based on a comprehensive evaluation.
- Provisional Certification: This is awarded to gateways that are lacking compliance in some non-critical aspect(s) of design, policy or management. It does not preclude the gateway from operating, but does mandate that the provisions be corrected within a specified timeframe.
- Recertification: This should be undertaken on all certified gateways at least every 12 months or at initiation of a major change.

Gateway Development Process

14. The development process focuses on a number of related issues, specifically a review of:

- risk assessment
- security policies
- design
- installation and configuration
- security management plans and procedures

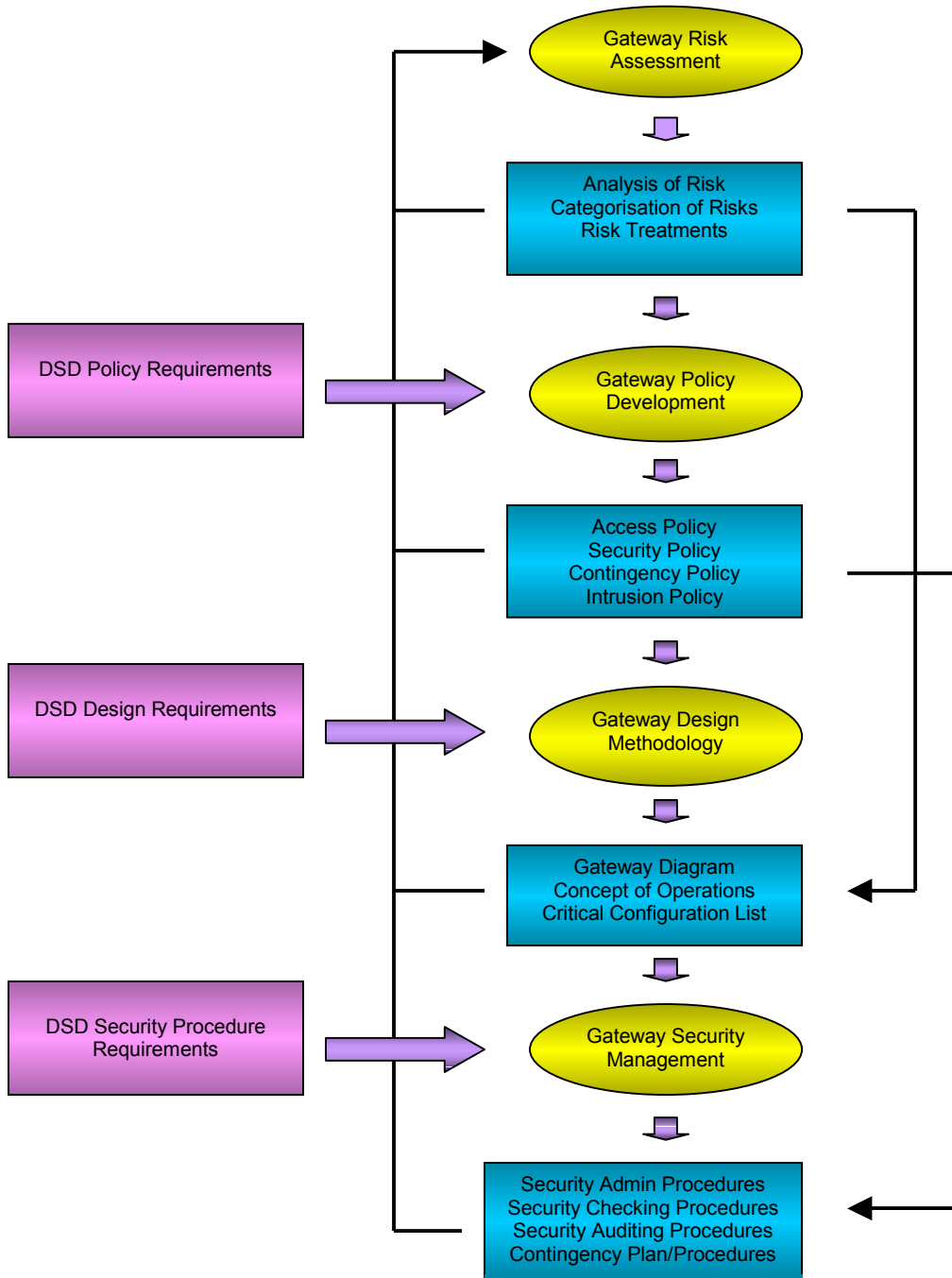
15. The titles of the documents given in this guide are guidelines; organisations may title their policies sections/documents as appropriate. To assist the certification process a document providing a map between the titles given in this document and the titles used by an organisation must be submitted during certification.

16. The function of gateways has expanded from the provision of traditional security services to include e-business, information services, and virtual private networks. The services provided from within the gateway infrastructure must attract the same management procedures as critical gateway components.

17. As part of the certification process, the assessor will specifically look for gaps and inconsistencies, adherence to minimum standards, mapping of the results of the risk assessment to the design and operation of the gateway, and realistic and achievable plans and procedures.

UNCLASSIFIED

18. This guide covers all the steps in the design and development process as illustrated by the following flowchart:



UNCLASSIFIED

1.0 Gateway Risk Assessment

19. The requirements contained in the following section are derived from ACSI 33 Part 2, Chapter 4.

20. Risk management is a process for comprehensively and systematically managing risk in an organisation. Gateway security risk management follows the same principles and processes as risk management, but the risks are specific to gateway security.

21. The Risk Assessment (RA) is an important component of an organisations risk management.

22. The organisation **MUST** conduct a RA on the gateway environment.

23. A RA **MUST** contain:

- analysis of the risks;
- categorisation of the risks including target risk levels/predetermined standards; and
- risk treatments.

24. The RA **MUST** have been signed by the CEO or delegate of the organisation confirming they have read and accepted the RA, including the identified residual level of risk.

UNCLASSIFIED

2.0 Gateway Policy Development Process

25. The Gateway Policy comprises high-level statements that describe the functional requirements and the association protects for the gateway. Assessors undertaking a certification of the gateway will be specifically looking for realistic policies that can and are implemented as part of the gateway management and operation.

26. The Gateway Policy has a number of components including the Access, Security, Contingency, Incident Detection and Response, and Configuration Control. These components can be either separate policy documents, or sections within one Gateway Policy document.

27. These policy statements need to clearly detail the key policy objectives and responsibilities.

2.1 Access Policy

28. The requirements contained in the following section are derived from ACSI 33 Part 3, Chapter 6.

29. Access Policy **MUST** ensure that:

- all gateway users (including groups), clients, or any subset are documented; and
- all services are denied by default unless expressly permitted.

30. Customer security requirements and the business requirements of the organisation will impact on the need to control access to services on a gateway. This may be either through a formal legal framework, or an internal security arrangement.

31. Access Policy **SHOULD** ensure that:

- access between networks, especially those networks that are owned by different organisations are documented;
- changes to the Access Policy will result in a review of the RA; and
- changes in business requirements will be reflected in policy and procedures.

32. There **MUST** be a clear correlation between the RA and the Access Policy.

2.2 Security Policy

33. The requirements contained in the following section are derived from ACSI 33 Part 3, Chapters 1, 2, 4, 6, 8 and 9.

34. Security Policy needs to detail the management of various security aspects of the gateway.

35. There **MUST** be a clear correlation between the RA and the Security Policy.

36. Security Policy **MUST** include:

- administrative security policy (ACSI 33, Part 3, Chapter 6);
- personnel security policy (ACSI 33, Part 3, Chapter 2);
- physical security policy (ACSI 33, Part 3, Chapter 1);

UNCLASSIFIED

- key management policy (ACSI 33, Blocks 3.9.35 to 3.9.50);
- hardware security policy (ACSI 33, Part 3, Chapter 4); and
- change management policy (ACSI 33 Blocks 2.8.6 to 2.8.12).

37. Administrative security policy **MUST** ensure that:

- the maximum classification of data handled or accessed by users and clients is documented;
- the responsibilities of users within the gateway and the training requirements of those users are established and documented;
- rules defining user account permissions and administration (including privileged users) are documented;
- the classification scheme is as per the definitions in the Protective Security Manual; and
- the data owner(s) are documented.

38. Personnel security policy **MUST** ensure that:

- users' security clearance requirements are documented;
- records of the status of users' security clearances are kept; and
- gateway premises access restrictions on personnel are documented.

39. Personnel security policy **SHOULD** ensure that legal conditions obligated on employees and contractors are documented.

40. Physical security policy **MUST** ensure that:

- all server rooms have a physical security certification to the appropriate server room standard for the system classification; and
- server room certification is performed by a suitable Certification or Accreditation Authority.

41. Key management policy **MUST** ensure that the cryptography used to protect classified information and systems is:

- approved by DSD; and
- is used in accordance with the standards outlined in ACSI 33..

42. Hardware security policy **MUST** ensure that:

- classification labeling and registering of hardware;
- the method for secure disposal and maintenance of hardware is documented; and
- media sanitisation and destruction is documented.

43. Change management policy **SHOULD** ensure that:

UNCLASSIFIED

- authorities for approving change are documented;
- Accreditation Authority approves changes that could impact the security of gateway; and
- associated system documentation will be updated to reflect changes.

2.3 Contingency Policy

44. The requirements contained in the following section are derived from ACSI 33 Part 2, Chapter 8.

45. There **MUST** be a clear correlation between the RA and the Contingency Policy.

46. The Contingency Policy **MUST** ensure that the critical management objectives for a contingency plan are documented.

47. The Contingency Policy **SHOULD** ensure that:

- a definition of an "incident" is documented;
- definitions of outages, and the authority responsible for declaration of each grade of an outage are documented;
- recovery time objectives, for the various grades of outages are documented;
- testing regime objectives and reporting of status of backup systems are documented; and
- on-line and off-line redundancy are documented.

48. An incident may not necessarily directly lead to an outage, but may require judgement to be exercised by a responsible authority.

49. The results of the RA **SHOULD** be used to provide guidance for required recovery times. In particular, DSD **RECOMMENDS** that specific attention be paid to prioritising system importance, determining achievable recovery times, allowing maximum flexibility for the management team in the event of an outage.

2.4 Incident Detection and Response Policy

50. The requirements contained in the following section are derived from ACSI 33 Part 2, Chapter 8.

51. These policy statements could have been covered either by the Security or Contingency Policy. However, DSD **RECOMMENDS** that it be addressed separately to reflect its importance in the management of a secure gateway. A security incident, in ICT terms, is an event that impacts on the confidentiality, integrity or availability of a system through an act of unauthorised access, disclosure, modification, misuse damage, loss or destruction.

52. Incident Detection and Response Policy **SHOULD** include the following components:

- detecting security incidents;
- managing security incidents;
- reporting of incidents; and
- incident response plan.

UNCLASSIFIED

53. Incident Detection and Response Policy **SHOULD** ensure that, for detecting security incidents, definitions on the types of incidents that are likely to be encountered are documented. As a guide, see the DSD website: http://www.dsd.gov.au/infosec/assistance_services/incident.html, for the types of incidents and how they could be categorised.

54. Incident Detection and Response Policy **MUST** ensure that for managing security incidents:

- the process for internal reporting of security incidents is documented;
- incidents are recorded and logged;
- possible data spillage is minimised; and
- malicious code is mitigated against.

55. The policy surrounding data spillage **SHOULD** assume that the information has been compromised. When data spillage has occurred it can be difficult to establish if the data has been compromised, therefore the policy needs to ensure the organisation responds appropriately. Policy that assumes data has been compromised will provide the organisation with a response procedure that is suitable for data spillage incidents.

56. The policy for handling malicious code **SHOULD** address:

- isolation of infection;
- anti-virus software to remove the infection; and
- measures to prevent further outbreaks.

57. Incident Detection and Response Policy **MUST** ensure that for the reporting of security incidents:

- DSD and connected gateway customers are addressees on off-line, analytical reports;
- analytical reports are sent at least quarterly to DSD and connected gateway customers;
- DSD is notified as soon as practicable of all Category 3 or higher incidents (as defined in ISIDRAS);
- DSD is informed of incidents that require formal investigative action; and
- users and clients are regularly informed on how to report security incidents to their Information Technology Security Administrator (ITSA) or equivalent in accordance with organisational procedures.

58. Incident Detection and Response Policy **SHOULD** ensure that for reporting of security incidents:

- timely reporting is done via the ISIDRAS reporting scheme;
- DSD and connected gateway customers receive all reports in the identified timeframe; and
- if necessary, the report is formally acknowledged or reported to a higher level.

59. DSD **RECOMMENDS** that the policy for reporting of security incidents define the regularity for producing analytical reports, what category of incident would be reported and who would receive the

UNCLASSIFIED

reports.

60. Incident Detection and Response Policy **MUST** ensure that the incident response plan:

- is based on the incident grading definitions;
- the response procedures are realistic and achievable, and identify the categories of incident to be reported on a timely basis; and
- agencies keep records of incidents for no less than 12 months.

61. Archive logs **SHOULD** be stored securely off-site. DSD **RECOMMENDS** that this includes how often the logs would be archived, how long they would be stored, whether they would be backed up, and whether the backups would be stored off-site.

62. DSD **RECOMMENDS** that mechanisms be in place to quantify and monitor security incidents and malfunctions, including types of incidents, costs of incidents and frequency of incidents. To support learning from incidents DSD **RECOMMENDS** that organisations maintain security incident statistics. DSD **RECOMMENDS** that organisations commit to regular reviews of security incident statistics in order to address organisation security risks, assist in the ongoing development of the organisation Security Plan and to provide a periodic feedback loop to the review of the Risk Assessment.

3.0 Gateway Design Methodology

63. The design of the gateway is critically important to the security of those services offered as part of the gateway implementation, and to those networks being protected by the gateway. This chapter details the design requirements for the implementation of gateways protecting Government information or networks.

64. This section details minimum requirements. The environments surrounding gateways differ between organisations. For this reason organisations have to take into consideration any additional requirements for their gateways design that have been identified in their risk assessment.

3.1 Gateway Major Components

65. The requirements contained in the following section are derived from ACSI 33 Part 3, Chapter 3.

66. The firewall is a central component of the gateway. The mandatory firewall **MUST** be a DAP and **SHOULD** be configured in accordance with the security target and certification report.

67. Figure 3.1 illustrates the gateways major components. The untrusted network is usually the Internet, but may be any network not in direct control of the organisation. The DMZ, contains the proxy servers or application firewalls required to provide security services at the application layer. The firewall in the figure is being used as a bastion host.

UNCLASSIFIED

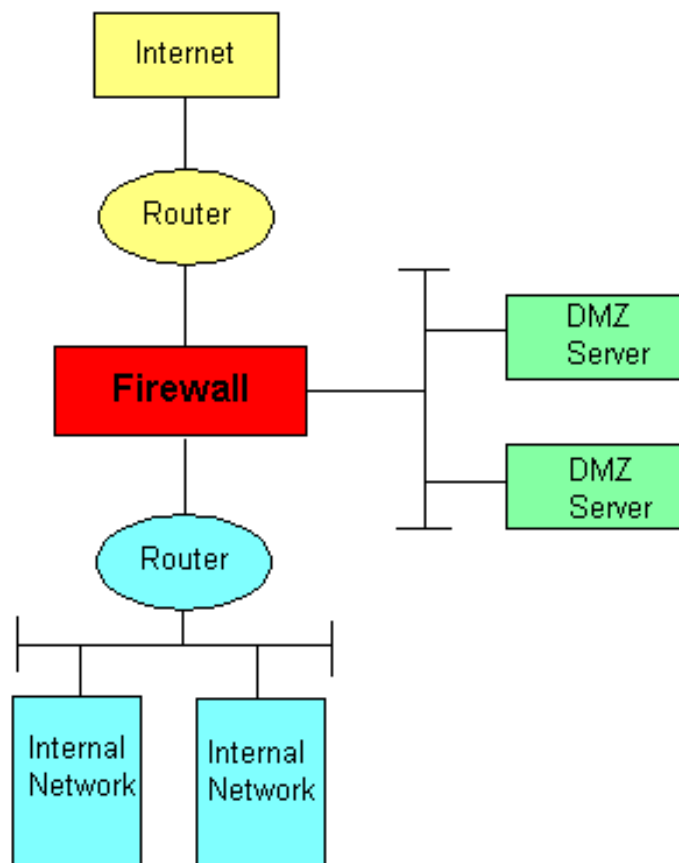


Figure 3.1: Major Components of a Gateway

68. Not all firewalls that support multiple interfaces provide trusted separation between those interfaces. This would be required if the firewall was being used to service multiple customers. Designers **SHOULD** ensure that the functionality required to provide interface separation is part of the evaluation of that firewall. Figure 3.1 shows a gateway with only one internal network connection, and only one DMZ. Multiple internal networks or gateways serving a variety of customers may need to ensure network separation. This may be accomplished by connecting extra customers to a multiple port firewall, as shown in Figure 3.2. This figure also demonstrates the use of multiple DMZs and is discussed later in the chapter. Note that multiple firewalls are not always required to service multiple customers.

69. In both Figure 3.1 and 3.2, further protection can be afforded to the internal network by using 2 firewalls. This protection is achieved by placing the first firewall after the border router and then connecting the DMZ to it. The second firewall is the link between the DMZ and the internal network. This second firewall can be locked down more tightly, thus giving the internal network more protection.

UNCLASSIFIED

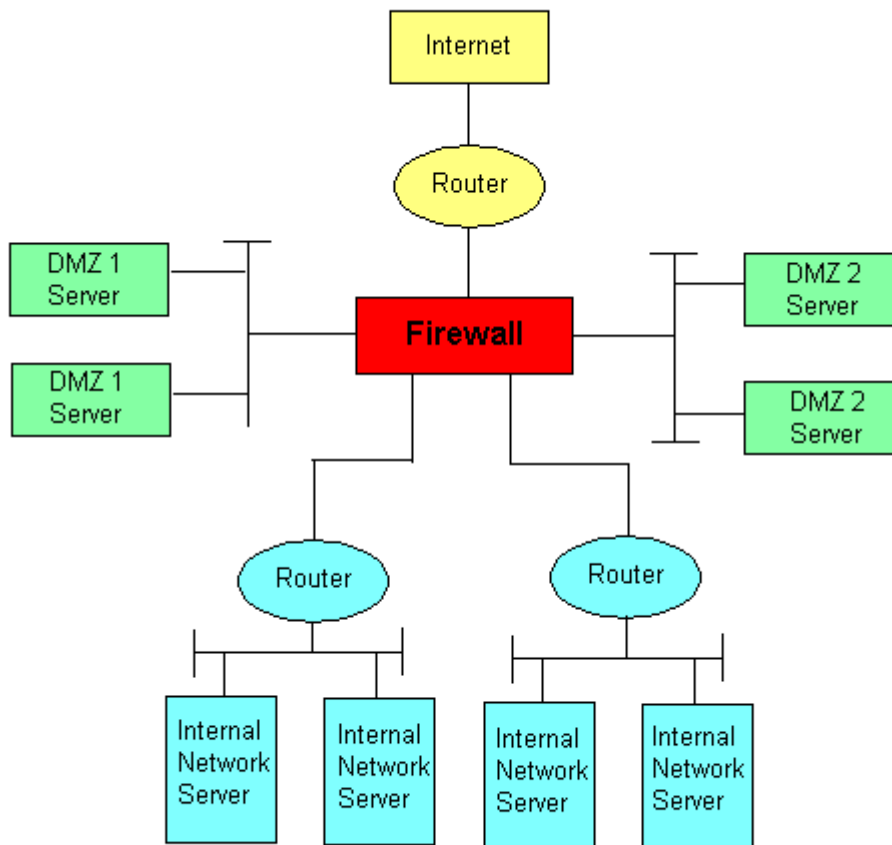


Figure 3.2: Major Components, Multiple User Gateway

70. In the event that the firewall of choice does not have enough interface connections, another evaluated firewall may be chained to provide security services to other internal networks.

71. Services that may require protection include dial-in, wireless connections etc. The protection of services provided by the gateway **SHOULD** be based on:

- the function of the service;
- the classification of the data;
- the data the service could have access to (eg other networks); and
- known vulnerabilities of the service that could be exploited and the impact of their exploitation.

3.2 Mandatory Security Design Criteria

72. The requirements contained in the following section are derived from ACSI 33 Part 2, Chapter 7 and Part 3, Chapter 10.

73. This section details those requirements for certification of a gateway. These requirements must

UNCLASSIFIED

be followed **regardless** of the outcomes of the risk assessment.

74. Network traffic to any device on either the internal network or the DMZ **MUST** be denied by default.

75. Access to services between multiple internal networks (if any) using the firewall (see Figure 3.2) **MUST** be denied by default. This is to prevent inadvertent access to a network by another customer network, where that access has not been specifically authorised.

76. All traffic traversing between networks **SHOULD** be routed through the gateway (including firewall(s)). The intention of this requirement is to avoid the situation where the security services offered by the gateway are negated by an insecure connection to another network with a different risk profile. Alternatively, the internal network connection may have a number of public connections each secured by an approved gateway, although this approach is not recommended due to resource overheads. Organisations **MUST** understand the risks associated with all external connections and have documented strategies to treat these risk.

77. All implementations of cryptographic services in the gateway, including those for confidentiality, authentication, non-repudiation or data integrity **MUST** be included within the scope of the gateway certification. Any cryptographic products used in the gateway environment **MUST** be a DACP or a DAP appropriate to the classification level of the gateway. A maximum certification level of provisional may be granted for gateways using DAPs that are in evaluation.

78. All communication links between the internal network components and the firewall, where the communications path is not physically controlled by agency and contractor staff (eg. a connection via a telecommunications carrier to a remote site providing gateway services) **MUST** be protected by a DSD approved method.

79. Firewall management **MUST** be provided via a secure path. This could be via a physically secure dedicated management console with well-managed identification and authentication mechanisms, or via an encrypted tunnel through the internal or external network. If a remote management feature is used, it **SHOULD** have been part of the product's evaluation.

80. Services **SHOULD NOT** be passed directly from the outside network to the inside network. All services available to outside users, except for encrypted services, **SHOULD** be proxied through the DMZ servers.

81. The internal and external border router(s) (refer Figure 3.1 or 3.2) **SHOULD NOT** be relied upon for access control. If appropriate, some firewall access controls could be copied to border routers to filter low category attacks.

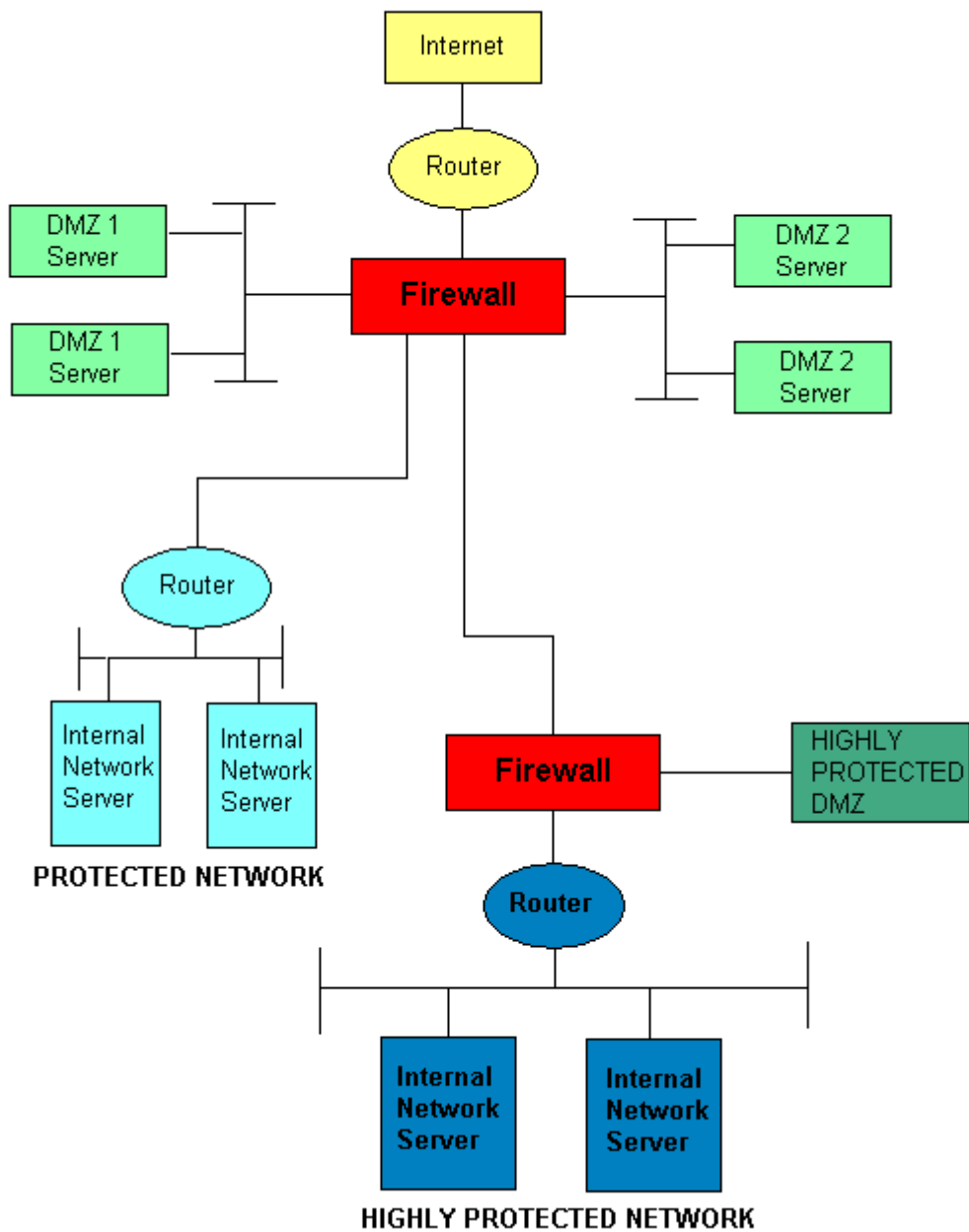


Figure 3.3: Multiple User Gateway, Serving PROTECTED and HIGHLY PROTECTED Networks

82. Figure 3.3 shows a possible configuration for HIGHLY PROTECTED gateway. The firewalls shown in the figure needs to be evaluated to at least EAL4 or E3 and from different manufacturers.

3.3 Risk Based Security Design Criteria

83. The requirements contained in the following section are derived from ACSI 33 Part 3, Chapters 7 and 10.

UNCLASSIFIED

84. This section details those gateway design aspects that should be based on the outcomes of the RA. There **MUST** be a clear correlation between the RA and the gateway design.

85. Security services available on gateway servers will be protocol specific, and **SHOULD** be determined by business requirements and the RA. Subject to the outcome of a RA, the following are examples of common services that may need to be protected by application level security measures:

- DNS: Name server on the DMZ with limited knowledge of the internal network addresses.
- Email: Virus detection software should be executed on all incoming and outgoing mail.
- Web: Java applets to be blocked.

86. The business continuity strategy for the gateway **MUST** be based on the policy. The extent of the strategy will be dependent on the system design, including the redundancy built into the system. Log backups **SHOULD** be treated differently if evidence/forensic capabilities for the data contained in these logs is required. Archive, storage and management of audit logs **SHOULD** reflect the requirements of the Incident Detection and Response Policy/Plan. DSD **RECOMMENDS** organisations consider on-line redundancy, as well as contingency planning. The outcome of the Contingency Policy **SHOULD** be used to determine availability requirements especially the balance between on-line and offline redundancy.

87. Auditing or logging services **MUST** be used to:

- monitor the real level of threat;
- provide real time alarms to critical events; and
- monitor the privileged users within the gateway.

88. The results of the Incident Detection and Response Policy, detailed in Chapter 2, **SHOULD** drive the requirements for auditing or logging. Logs **SHOULD** also be provided to monitor the administration of the gateway. The degree of audit information to be collected will be a function of the resources available to collect and process this information and the degree to which it is intended to mitigate identified risks. It is important that the gateway designer critically examine how audit information may be collected, processed and analysed. The information contained in logs **SHOULD** be reviewed within a time frame as described in the Incident and Detection Response Policy and critical patterns identified to form the basis of exception reporting.

89. The following events **SHOULD** be logged for the firewall, DMZ servers and other critical components, for both successful and unsuccessful attempts:

- logon and logoffs;
- boot and initialisation;
- shutdown, and associated details;
- restart, and associated details;
- changes to the firewall configuration;
- policy exceptions;

UNCLASSIFIED

- password changes;
- TCP/UDP/ICMP connection requests; and
- application connection type, and data volume transferred.

90. For each event that is logged, the following information **SHOULD** be logged, in order to meet the requirements of the IDRPs:

- event name or description;
- date and time;
- account Id;
- command parameter;
- IP source and destination address;
- protocol code or description; and
- source and destination port.

3.4 Critical Security Configuration

91. Security management processes designed to ensure the integrity of the gateway help to achieve the desired level of protection. While the proper configuration of the firewall at installation is important, the business processes used to pinpoint problems, correct errors, detect misconfigurations, respond to changes in threat, cater for maintenance issues and allow for changes in personnel are crucial to the gateway design. The users responsible for drafting the plans and procedures need to know, or be aware of, the critical configurations.

92. The following issues **SHOULD** be addressed:

- **System backup configuration.** The specific components of the gateway that need to be backed up and how this will be achieved.
- **System device configuration.** The configuration of critical devices used by the gateway needs to be specified in the critical configuration list. Users are best placed to identify a list of those items that require strict configuration controls, as determined in part by the risk assessment process. The list includes:
 - Firewall access lists
 - Firewall management configuration
 - Encrypted modem configuration, including key management issues
 - Web proxy server configuration

3.5 Design Documentation

93. The design documentation **MUST** include the following components:

- **Gateway logical/infrastructure diagram.** A diagram showing the components of the gateway.

UNCLASSIFIED

- **List of requirements.** A detailed list of the design requirements mapped against controls put in place to meet the requirement. This list needs to include requirements that have been identified as a result of the risk assessment.
- **List of critical configurations.** These are the list of critical configurations to ensure integrity of the gateway operating environment. The following configurations files are required to be provided to the Certification Authority:
 - firewall configuration;
 - proxy server configuration file;
 - audit file; and
 -
 - account profiles.
- **Detailed configuration documentation.** These are the configuration files (including versions) for the critical configurations.

4.0 Gateway Security Management

94. The ongoing secure management of the gateway is paramount to ensuring a secure operating environment. Sound security business processes flow from a considered security management framework, and it is the intention of this chapter to detail the management tools necessary for a certified secure gateway.

95. The terms "plan" and "procedure" are used throughout this chapter. The term "plan" is used to refer to documentation that may detail the configuration, framework or requirements of a specific item. The term "procedure" is used to detail exactly how a task is to be undertaken, including the tools to be used, the commands to be executed, and the privileges to be held.

96. The key objectives that influence the tasks of the security administrators can be broken down into a number of distinct components:

- Security administration tasks;
- Proactive security configuration checks;
- Proactive security audit checks; and
- Contingency plans and tasks.

97. There **MUST** be a clear correlation between gateway policy and all the plans and procedures. For gateway management there **MUST** be demonstrated evidence of implementation of all the plans and procedures.

98. The effort that will be spent on each of the components listed above depends on the RA, the configuration of the gateway and the tools in use by the system administrator team. The remainder of this chapter details the broad requirements that need to be addressed under each of the components listed above.

99. DSD **RECOMMENDS** that the plans and procedures drafted be brief and concise. Procedures **SHOULD** be readily available for operators and administrators to utilise in the event of a system outage or compromise. They can also be stored on-line in a secure environment.

4.1 Security Administration Tasks

100. The requirements contained in the following section are derived from ACSI 33 Part 3 Chapters 2, 3, 4, 6 and 9.

101. The security administration tasks include all the "day to day" tasks that are typical of any IT installation. They need to cover the completion of stated tasks including by whom, under what specific authority, following what specific processes, in what timeframe and any records that need to be maintained.

102. The security administration tasks **MUST** include:

- accounts administration plan and procedure;
- privileged user plan and procedure (ACSI 33 3.6.20);
- access control plan and procedure(ACSI 33 3.6.30);
- key management plan (ACSI 33 Part 3, Chapter 9);

UNCLASSIFIED

- user awareness plan (ACSI 33 Part 3, Chapter 2);
 - hardware security plan and procedure (ACSI 33 Part 3, Chapters 3 and 4); and
 - change management plan and procedure (ACSI 33 Part 2, Chapter 8).
103. Accounts administration plan and procedure **MUST** detail:
- profile of system accounts;
 - users allowed an account;
 - removal of old accounts; and
 - outline of account administration record keeping.
104. Privileged user plan and procedure **MUST** detail:
- privileged accounts; and
 - who holds is allowed to hold privileged accounts.
 - how privileged accounts are controlled and accountable;
 - rules on privileged accounts (for example, administrators are assigned individual accounts to ensure all admin tasks are accountable); and
 - definition on type of work allowed to be performed on privileged accounts (for example no privileged accounts can be used for non-administrative work).
105. Access control plan and procedure **SHOULD** detail:
- the users (including user groups);
 - allocated/allowed resources;
 - how users' access is limited;
 - how to perform access control changes; and
 - who can authorise access control changes.
106. Key management plan and procedure is mandatory only where cryptographic services are employed as part of the gateway.
107. Key management plan and procedure **MUST** detail:
- how keys are derived;
 - how often they are changed for each system;
 - users that are allowed access; and
 - actions to be taken in event of compromise or replacement.
108. Hardware security plan and procedure **SHOULD** detail:
- systems requiring backup;

UNCLASSIFIED

- frequency of backup;
 - period of storage;
 - media reuse/disposal; and
 - archival of logs or audit trails.
109. User awareness plan **SHOULD** detail:
- processes for initiating and maintaining a program so users are aware of their responsibilities;
 - processes to ensure training programs are aligned with user responsibilities; and
 - the appropriate activities for use of the services and safe practices for use of the services.
110. The change management plan and procedure **MUST** contain:
- stakeholders in the change process;
 - the responsibilities for approving changes to systems;
 - the process by which changes are approved;
 - the communication of change details to all relevant persons; and
 - the records to be maintained.

4.2 Proactive Security Checking Tasks

111. The requirements contained in the following section are derived from ACSI 33 Part 3, Chapter 7.

112. Proactive security checking is often an overlooked component of the overall security strategy of a system, yet it is fundamental to providing a degree of assurance that the security configuration integrity is intact.

113. The proactive security checking tasks **MUST** detail:

- those responsible for checking the gateway system;
- the components that will be checked and by what means (i.e. whether tools are required);
- how often these checks are to be undertaken; and
- the authority that is to receive the reports.

114. The configuration items that require checking and the regularity of checking **MUST** be derived from the critical configuration list and the relevant Security Policy.

115. DSD **RECOMMENDS** that reports be by exception, however a log of checking activity should be maintained for audit purposes. The assessor will pay particular attention to the reports, to ensure

UNCLASSIFIED

they are readable and do not place an undue burden on the recipient. The proactive security checking tasks **MUST** include:

- firewall configuration checking plan and procedure;
- proxy server configuration checking plan and procedure;
- cryptographic configuration checking plan and procedure; and
- alarm and access control plan and procedure.

116. The plan and procedure for each of the above areas **SHOULD** detail:

- items that need to be checked;
- what tool will be used to check them;
- what checksum algorithm is being used;
- how often this will be undertaken;
- how the reporting is to be undertaken;
- the appointment(s) responsible for checking; and
- who should receive the reports.

117. The cryptographic configuration includes cryptographic information associated with remote management, Virtual Private Networks (VPNs), Public Key Infrastructures (PKIs), link encryptors, smartcards or cryptographic tokens, etc. This document is conditional on whether these cryptographic systems are employed as part of the gateway.

118. The alarm and access control plan and procedure is conditional on whether there is an electronic or semiautomatic physical entry access control, or an alarm or physical detection system

4.3 Proactive Security Audit Checks

119. The requirements contained in the following section are derived from ACSI 33 Part 3, Chapter 7.

120. Proactive security audit will alert the security administrators to an increased level of threat against a particular service, component or user on a gateway. It is important that the administrators are not only aware of the threat level, but also use this information to deal with the subsequent security issues in a proactive, timely manner.

121. DSD **RECOMMENDS** that reports be by exception, so as not to overload the recipient of the report with an inordinate amount of material to analyse. The assessor will pay particular attention to the reports, to ensure they are readable and do not place an undue burden on the recipient. The documentation for proactive security audit **MUST** include timely reporting and off-line or analytical reporting plans and procedures.

122. The plan and procedure for each of the above areas **MUST** detail:

- who is responsible for checking the audit trails;
- the specific objectives of the checking;

UNCLASSIFIED

- the tools that would be used for this function (if any);
- how often these checks should be undertaken; and
- the appointment that is to receive the reports.

123. The information required for these tasks **MUST** be derived from the outcomes of the gateway design and the relevant security policy.

124. The objective of the real-time reporting is to ensure there is a plan and procedure to alert the security administrators, in real time, of those events that pose a direct threat to the integrity of the gateway.

125. The objective of the off-line analytical reporting is to ensure there is a plan and procedure to provide the security administrators and management with an indication of the level of threat or attack being experienced by the gateway.

126. DSD **RECOMMENDS** this information is used, in time, to further develop the RA by providing more realistic metrics on the actual threat likelihood.

4.4 Contingency Plan

127. The requirements contained in the following section are derived from ACSI 33 Part 2, Chapter 8.

128. The Contingency Plan **SHOULD** describe the plans and procedures to be followed in event of an actual contingency, including how the plan is to be checked and monitored.

4.5 Incident Detection and Response Plan and Procedure

129. The requirements contained in the following section are derived from ACSI 33 Part 2, Chapter 8.

130. Organisations **SHOULD** develop and maintain procedures in addition to the incident response plan that:

- detect potential security breaches;
- establish the cause of any security incident, whether accidental or deliberate;
- detail the action required to recover and minimise the exposure to a system compromise;
- assist in reporting the incident. (e.g. use of ISIDRAS); and
- promote prevention of incidents and limit recurrences of incidents.

131. These could be covered in the contingency plan or separately. The incident detection and response plan and procedure **MUST** describe the steps to be followed when the proactive security checking tasks and audit tasks identify a security incident.

132. Identified actions (eg. disconnecting the gateway) **SHOULD** map to the incident categories identified in the incident detection and response policy.

133. Incident investigation, reporting, evidence preservation, media control and recording, and system recovery procedures **SHOULD** to be outlined in relation to each category of incident.

UNCLASSIFIED

134. The appointment(s) responsible for performing incident response also **MUST** be clearly identified.