Australian Government

Department of Defence

Defence Signals Directorate

GATEWAY CERTIFICATION GUIDE

VERSION 3.0

Point of Contact: Advice and Assistance Group

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

Table of Contents

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, whether the systems process nationally or non-nationally classified information or even unclassified information.

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 agency connects to an untrusted network. The large number of threats to systems, data and applications, and the high or even extreme level of threat likelihood dictates that appropriately managed safeguards are required to protect agency information systems so as to minimise the risk of intrusion to or compromise of these systems.

Purpose and Scope

3. The Gateway Certification process aims to provide an Australian Government agency, or a Service Provider to Australian Government agencies with an independent assessment that their gateway has been configured and managed to industry and Australian Government best practice, and that appropriate safeguards are implemented and operate effectively.[1] This assurance provides clients using the gateway services with a level of trust in the service provided. This guide is designed to assist agencies seeking certification, including recertification.

4. This Guide also serves as a reference detailing the areas of specific concern to the assessors conducting the certification and allows agency or company staff to scope, cost and resource the security requirements in advance of the certification process itself. Accordingly, this document could provide a reference for independent "verification" of any gateway.

5. This document **SHOULD** be used in conjunction with the Australian Government IT 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), can also assist in preparation for certification.

[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 best practice standards. A Gateway Certification performed by an I-RAP assessor for gateways classified up to PROTECTED is recognised by DSD.

Keywords

6. The table below defines the keywords used within this document to indicate the level of requirements for DSD or I-RAP certification. All keywords are presented in bold, upper-case format.

Keyword	Interpretation
MUST	The item is mandatory if seeking certification.
MUST NOT	Non-use of the item is mandatory if seeking certification.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. **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, but the full implications need to be considered before choosing this course. **Note:** Agencies deviating from a **SHOULD NOT**, **MUST** document the reason(s) for doing so.
RECOMMENDS **RECOMMENDED**	The specified body's recommendation or suggestion. **Note:** Agencies deviating from a **RECOMMENDS** or **RECOMMENDED**, are encouraged to document the reason(s) for doing so.

7. A **gateway** is a secured connection between networks, including connections to untrusted networks such as the Internet, or connections to other agencies or systems within the one agency. It will usually comprise of a number of components including firewall hosts, proxy servers, routers, email hosts, etc.

8. A **Demilitarized Zone** (DMZ) is a component of the gateway that contains those hosts that can be accessed directly by users on the external network. It therefore has some security, but is not completely trusted by the internal network.

9. A **firewall** is the host within the gateway designed to filter both incoming and outgoing data packets, and access to applications and data according to a set of configurable rules. A firewall can range in function from packet filtering, circuit level or application level gateway, authentication and encryption services.

References

10. This manual has been drafted with reference to the following publications:

- Commonwealth Protective Security Manual
- Australian Government Information Technology Security Manual also known as ACSI 33.

Gateway Certification Process

11. Gateway Certification is provided as an independent service to verify that a gateway is being managed to Australian Government and industry best practice. This certification process does not provide any guarantee that the gateway manager will always comply with minimum DSD requirements. However, checks will provide a degree of assurance that management processes are satisfactory for the continued, secure operation of the gateway.

12. The certification process performed by DSD or I-RAP assessors can be broken down into five distinct phases. See Part 2, Chapter 7 of ACSI 33 for more details.

Conditions of Certification

13. DSD will provide, on a fee for service basis, certification for gateway environments.

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

a. Advice to DSD on major changes to key components, including policy; **before** these changes are implemented.

b. Regular discussion with DSD on any changes to the analysed threat level.

15. **Provisional Certification** See Part 2, Chapter 7 of ACSI 33 for more details.

16. **Entry-Level Certification** is awarded to those companies or firms that wish to provide secure gateway services to Government agencies. This type of certification allows a company to seek Government clients, and is dependent upon an additional certification check within a short timeframe of a Government client being connected. This will be advised via the certification letter and report.

17. **Recertification** See Part 2, Chapter 7 of ACSI 33 for more details.

18. Australian Government service providers requiring certification **MUST** contact DSD for advice on the best way to achieve this certification.

Gateway Development Process

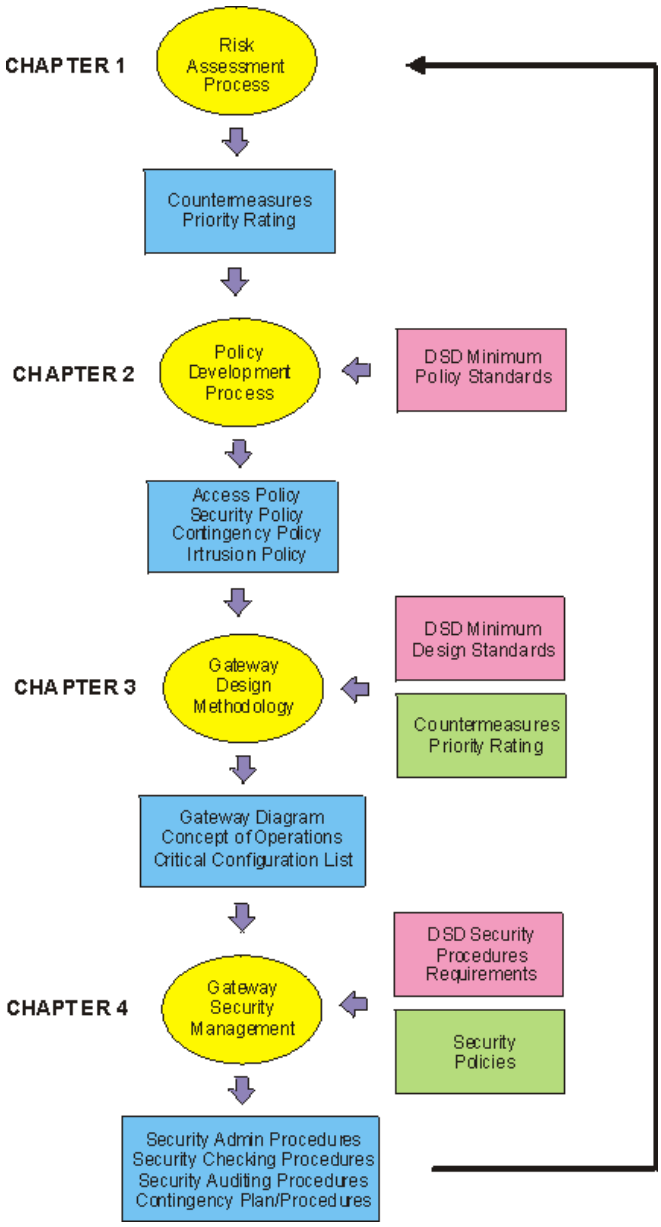
19. The development process focuses on a number of related issues, specifically a review of:

- The gateway risk assessment (Risk Management Plan (RMP))
- The gateway security policies (Information Technology Security Policy (ITSP))
- The gateway design
- The gateway installation and configuration
- The gateway security management plans and procedures. (System Security Plan (SSP) and Standard Operating Procedure (SOP))

20. As many gateways are operating as complex environments, the development process may not be limited to the above issues. 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 should attract the same management procedures as critical gateway components. Detailed discussion on the certification requirements are addressed in later chapters.

21. As part of the review, the assessor will specifically look for gaps and inconsistencies, indications that minimum standards have or have not been met, mapping of the results of the risk assessment to the design and operation of the gateway, and realistic and achievable plans and procedures.

22. This guide covers all the steps in the design and development process as illustrated by flowchart below.



Chapter 1
Security Risk Assessment

23. As a security tool, a risk assessment aims to provide a degree of assurance that the resource cost of security countermeasures used to counter specified threats is commensurate with the risks.

24. Gateway security risk management follows the same principles and procedures as risk management, but the risks are specific to gateway security.

25. A risk assessment **MUST** be conducted to provide guidance on the level of risk to be expected in the gateway environment.

26. The likelihood and consequence levels **MUST** be defined in the Risk Assessment.

27. The CEO or delegate of the agency / organisation **MUST** have signed off as having read and accepted the risk assessment, including the identified residual level of risk.

28. ACSI 33, in Part 2, Chapter 4, provides advice on risk management and the process of conducting a Risk Assessment.

Chapter 2
Gateway Policy Development Process

29. The Gateway Policy describes the philosophy by which the gateway is managed. 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. "Broad sweeping" security statements are discouraged from inclusion in these policies.

30. A number of gateway policy documents are required for certification. They are discussed in this chapter.

31. 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 the Gateway Policy, usually totalling no more than 10 – 15 pages. These policy statements clearly detail the key policy objectives and responsibilities. Details on how the gateway is to be managed and how policy issues are implemented are addressed in plans and procedures documents, and not in the policy documents.

Access Policy

32. The Access Policy **MUST** by default deny all services unless expressly permitted. This applies to both internally or externally generated connections. This policy **MUST** also detail which services are allowed, both for incoming and outgoing connections.

33. The results of the risk assessment **MUST** be used as the basis for detailing those services that will be allowed. However, customer security requirements and the business requirements of the organisation will also 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. In short, the results of the risk assessment, coupled with customer's requirements (if any) **MUST** be used to provide an Access Policy that details:

a. Those services available to all internally connected clients.

b. Those services available to all external users.

c. Those services to be denied or allowed on an individual, internal customer basis. Additionally, those services allowed or denied to external users on behalf of the agency.

d. Extra security services specified by individual clients either through a legal framework or other formal arrangement.

e. Access between networks, especially those networks that are owned by

different agencies. This **SHOULD** detail those services that are allowed between agencies, and any subsequent security requirements.

34. The Access Policy **SHOULD** include an outline of procedures for change to the policy. Changes in business requirements will be reflected in a change to the Access Policy, which should be accompanied by a review of the Risk Assessment process. These requirements **SHOULD** be formally referenced in the policy.

35. There **MUST** be a clear link between the Access Policy and the Risk Assessment, so that the Access Policy objectives and their associated countermeasures are appropriate to the level of identified risk.

Security Policy

36. The Security Policy needs to detail the management of various security aspects of the gateway. The results of the Risk Assessment are used to prioritise or focus efforts on those countermeasures that are important in mitigating identified risks. For example, if it is noted that a risk associated with "loss of information" through lack of controls on magnetic media may be a problem, then particular emphasis can be placed on controlling media by stating it as such in the Security Policy.

37. There **MUST** be a clear link between the Security Policy and the Risk Assessment, so that the Access Policy objectives and their associated countermeasures are appropriate to the level of identified risk.

38. The Security Policy can be divided into the following components:

a. **Administrative Security**. This section **MUST** detail the maximum classification of data that will be handled, or *could* be accessed by staff in the gateway environment. This **MUST** include the classification of data that will be accessed by outside users of the gateway. The classification scheme **SHOULD** be as per the definitions of the Protective Security Manual, for gateways that handle Government information. The data owner(s) **SHOULD** also be identified, in this policy item.

b. **Personnel Security**. This **MUST** detail the requirement for staff to be security cleared, and how this will be achieved. If no formal security clearance is required, detail the policy for background checking of staff to ensure inappropriate staff are not employed in the management of the gateway. Policy direction on which staff are allowed to enter the gateway premises, be given accounts on internal systems, and be given privileged accounts on gateway systems **MUST** be included. Legal conditions obligated on employees and contractors **SHOULD** also be included.

c. **Physical Security**. Detail the physical security objectives including (but not limited to) waste disposal, guarding, physical security alarms and response times, physical locks and physical security structure of all relevant premises. See Part 3, Chapter 1 of ACSI 33 for more details and contact T4

Protective Security of Australian Security Intelligence Organisation (ASIO) for the standards.

d. **Communications and Key Management Security**. Detail the policy objectives for handling and storage of cryptographic keys. Cryptographic keys can be those related to software or hardware based encryption systems. Control of these keys **MUST** be handled in the same manner as privileged accounts. See Part 3, Chapter 8 of ACSI 33 for standards.

e. **Equipment Maintenance and Disposal**. This section covers the policy objectives for ensuring that integrity of the gateway system hardware and software, and data confidentiality is maintained, when equipment is replaced or serviced. Policy objectives **SHOULD** include whether uncleared staff are allowed to maintain equipment, and if so how this would be achieved.

f. **Normal and Privileged Access to Systems**. Management **MUST** detail those staff or appointments that are allowed unsupervised access to the systems, which particular staff or appointments will be granted superuser or privileged access to specified systems, and which staff manage key or cryptographic systems.

g. **Media Security**. An important component of the overall security policy is that associated with handling, control, storage, declassification and destruction of media. This **SHOULD** include requirements for accountability of media within the gateway environment.

h. **Configuration and Change Control**. This **SHOULD** detail the responsibilities for approving changes to systems, and the process by which these changes are approved. Stakeholders in the change process **SHOULD** be defined. This policy item is not to be concerned with identifying at what level of detail a configuration change is identified, but rather the process by which these changes are to be efficiently and effectively handled. Include reference to the design documentation.

i. **User Responsibilities and Awareness**. This **SHOULD** detail the responsibilities associated with the use of the gateway system and the requirements for ensuring that users are made aware of their responsibilities.

j. **Agency and Service Provider Responsibilities** (if utilising a service provider). Where gateway services are provided by a service provider, the attribution of liability and acceptance of residual risk **MUST** be documented and understood by the agency.

Contingency Policy

39. The Contingency Policy **MUST** detail the critical management objectives for a contingency plan. A clear link between the Risk Assessment and the Contingency Policy **MUST** be established, so that the Contingency Policy objectives are appropriate to the level of identified risk.

40. The policy **SHOULD** deal with the following issues:

a. Definition of an "incident", and the authority responsible for declaration of an incident. An incident may not necessarily directly lead to an outage, but may require judgement to be exercised by a responsible authority.

b. Definitions of outages, and the appointment responsible for declaration of each grade of an outage.

c. Recovery time objectives, for the various grades of outages.

d. Testing regime objectives and reporting of status of backup systems.

e. On-line redundancy and off-line redundancy.

41. The results of the Risk Assessment **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.

Incident Detection and Response Policy

42. 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.

43. Clear definitions on the types of incidents that ***are likely*** to be encountered **SHOULD** be detailed, so that a documented plan can be derived to alert management to the expected response. 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.

44. The categories of incidents may not completely or exactly define each attack against a gateway. Indeed, some legitimate attempts to gain access may be viewed as an attempt to attack the gateway. Nevertheless, the grading of incidents is useful in determining a response policy and this **SHOULD** cover the following security objectives:

a. **Real-time reporting**. This **SHOULD** be specific, and based on the incident grading definitions. These objectives should be realistic and achievable, and include what category of incident would be reported on a real-time basis, who would receive the report and whether the reports need to be formally acknowledged or reported to higher levels. For DSD or I-RAP certified systems, DSD **MUST** be notified as soon as practicable of all Category 3 or higher incidents. This **SHOULD** be done via the ISIDRAS reporting scheme.

b. **Off-line or analytical reporting**. This **SHOULD** be specific, and based on the incident category definitions. DSD **RECOMMENDS** that this objective define the regularity for producing analytical reports, what category of

incident would be reported and who would receive the reports. DSD and connected gateway customers **MUST** be information addressees on off-line, analytical reports.

c. **Archiving of logs**. 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. Agencies **MUST** keep archives of logs for no less than 12 months, and these archives **SHOULD** be stored securely off-site.

d. **Authority responsible for initiating a formal (administrative) investigation and possible police investigation of an incident**. Note that this may overlap with some of the provisions of a Contingency Policy. DSD **RECOMMENDS** that this outlines the criteria by which the responsible authority would initiate a formal or police investigation of an incident, and which agencies or authorities would be informed in the event of an investigation being undertaken. DSD **MUST** be an information addressee on incidents that require formal investigative action.

e. **Incident Response**. Detail the response that is to be followed given expected, predicted or possible incidents.

Chapter 3
Gateway Design Methodology

45. 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.

46. The following diagrams depicting gateway components and network separations are not intended to be prescriptive architectures. The gateway architect **SHOULD** use risk based design criteria in order to develop the appropriate gateway architecture to suit the environment. Mandatory requirements **MUST** be incorporated into the design. Where possible, maximum flexibility has been afforded to the designer and the mandatory requirements have been kept to a minimum.

Gateway Major Components

47. Figure 3.1 illustrates the gateway major components. The untrusted network is usually the Internet, but may be any network. 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.

48. The central component of the gateway is the firewall, and it is for this reason that the firewall **MUST** be evaluated and configured in accordance with the security target and certification report to meet its particular standard. See Part 3, Chapter 9 of ACSI 33 for more details.

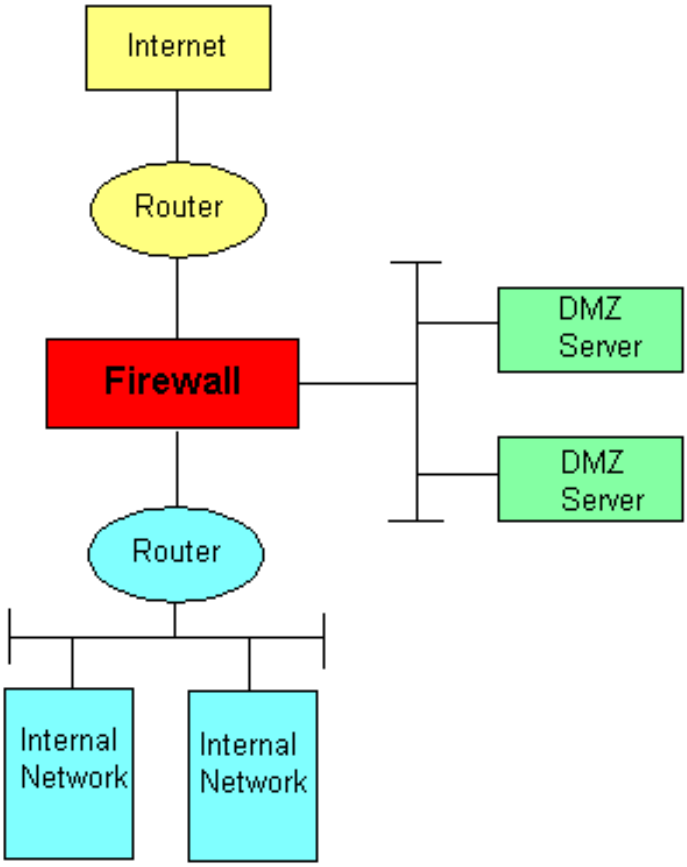


Figure 3.1: Major Components of a Gateway

49. 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 be protected from other networks. 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.

50. 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.

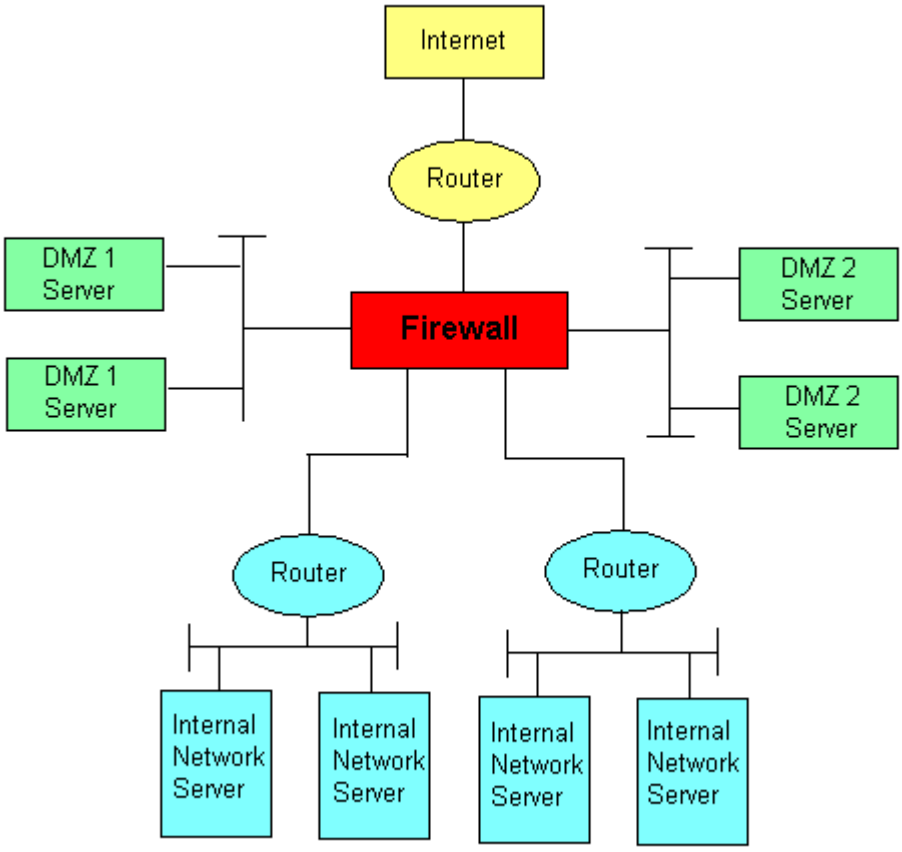


Figure 3.2: Major Components, Multiple User Gateway

51. 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. The DMZ may contain a number of servers.

52. Positioning of dial-in services, as well as other services provided by the gateway, **SHOULD** be subject to risk based design criteria which examines what data classification resides on these servers, what data is accessible by these services and whether the service has vulnerabilities which could be exploited to access other systems. For example, a dial-in service which provides access to the Internet connection to external dial-in users may be connected to the external router without posing a significant risk to other network components.

Mandatory Security Design Criteria

53. This section details those requirements that are mandatory for certification of a gateway. Accordingly, these minimum standards **MUST** be followed **regardless** of the outcomes of the risk assessment.

54. Incoming and outgoing services, to either the internal network(s) or the

DMZ, **MUST** be denied by default. This is a feature of most firewalls, although some configuration may be involved. In any case, this is the default policy that is required. Designers should note that this policy **MUST** also apply to the proxy or other servers on the DMZ, since this will minimise exposure to those servers and therefore services.

55. 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.

56. All traffic between the external and internal network **MUST** be routed through the firewall as the only route into and out of the internal network. The intention of this criterion is to avoid the situation where the security services offered by the gateway are voided by an insecure connection to the same public network. 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. The agency **MUST** have an understanding of all external connections that potentially bypass gateway safeguards, and have strategies for the security management of any such connections.

57. 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. Gateway designers **SHOULD** refer to the DSD Evaluated Products List for a selection of approved products and consult with DSD regarding the appropriate selection of cryptography for gateway services if there is any difficulty in complying with this policy.

58. 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.

59. Firewall management **MUST** be provided via a secure path. This could be via a physically secure dedicated management console with well-managed password-based identification and authentication system, 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.

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

61. The internal and external border router(s) (refer Figure 3.1 or 3.2) **SHOULD NOT** be configured for access control unless absolutely necessary. This is to allow service/connection requests to be passed to the firewall, to allow for all

successful and unsuccessful attempts at connection to be logged. If appropriate, some firewall access controls could be copied to border routers to filter low category attacks, however border routers **SHOULD NOT** be relied upon for access control.

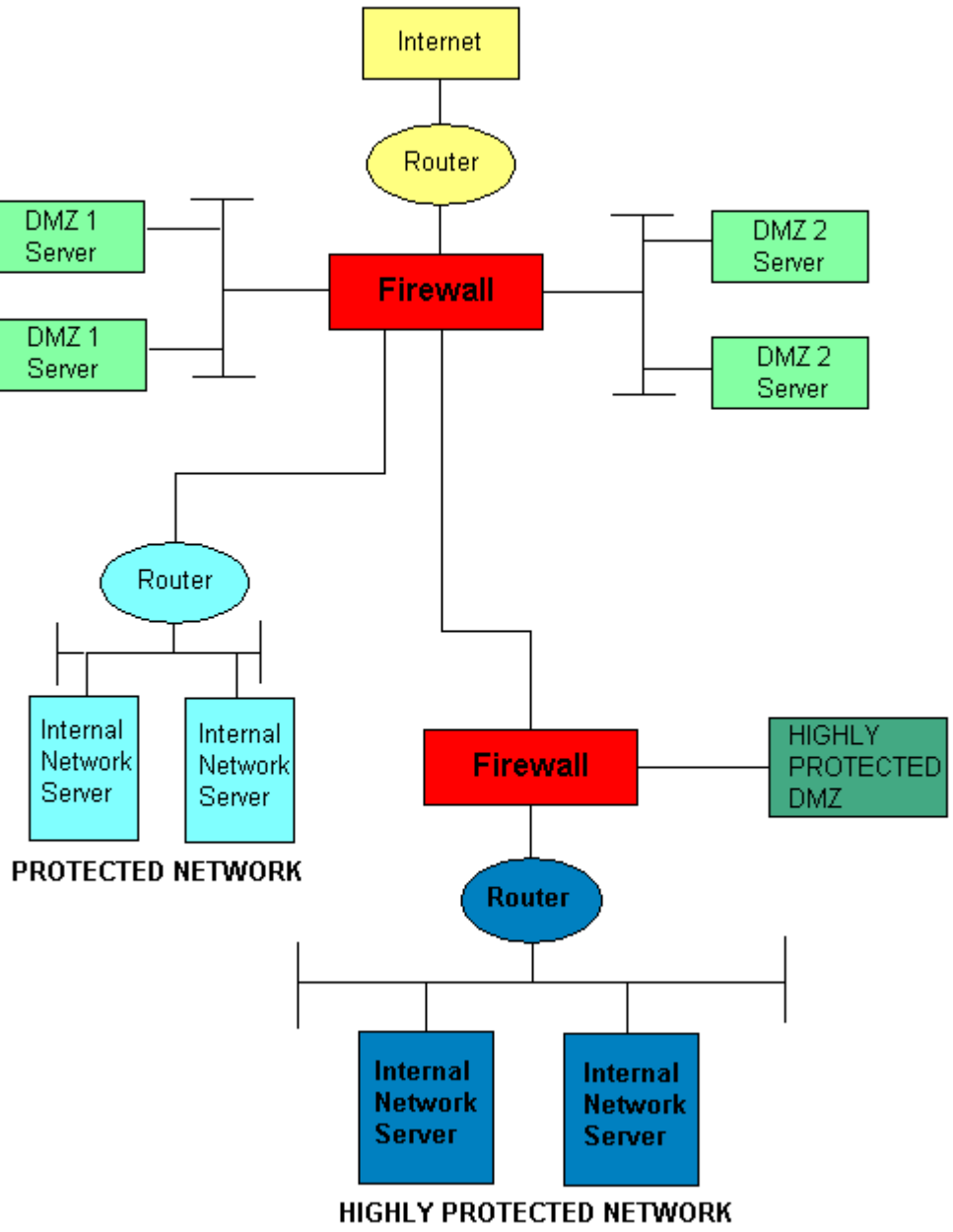


Figure 3.3: Multiple User Gateway, Serving PROTECTED and HIGHLY PROTECTED Clients

62. Figure 3.3 shows a possible configuration for HIGHLY PROTECTED clients.

For those gateways offering services to HIGHLY PROTECTED clients, the firewalls shown in the figure **MUST** be evaluated to at least EAL4 or E3 and **MUST** be from different manufacturers.

Risk Based Security Design Criteria

63. This section details those gateway design aspects that should be based on the outcomes of the risk assessment. There **SHOULD** be a clear linkage between the results of the risk assessment and the actual designed countermeasures established.

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

a. **DNS**. Name server on the DMZ with limited knowledge of the internal network addresses.

b. **Email**. Virus detection software should be executed on all incoming and outgoing mail.

c. **Web**. Java applets to be blocked.

65. Measures designed to mitigate risks to availability will greatly depend on the results of the risk assessment. DSD **RECOMMENDS** that agencies consider on-line redundancy, as well as contingency planning. The outcomes of the Contingency Policy, discussed in Chapter 2, **SHOULD** be used to drive those issues regarding availability, especially the extent and balance between on-line and off-line redundancy.

66. System backups, and the associated processes **SHOULD** be considered. The extent of backups will be dependent on the system design, including the redundancy built into the system. The Security Policy, discussed in Chapter 2, **SHOULD** be used for guidance. Audit log backups are 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.

67. Auditing or logging services **MUST** be used by Gateway management staff to monitor the real level of threat on a continuous basis and to provide real time alarms to critical events. Logs **SHOULD** also be provided to monitor the administration of the gateway. The results of the Incident Detection and Response Policy, detailed in Chapter 2, **SHOULD** be used to drive the requirements for auditing or logging. The degree of audit information to be collected will be a function of the resources available to collect and process this information. It is important that the gateway designer critically examine how audit information may be collected, processed and analysed. Over time, the information contained in logs should be reviewed and critical patterns identified

to form the basis of exception reporting.

68. The level of monitoring designed for the gateway **MUST** be based on the risk assessment, and may include the following events that occur on 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
- Password changes
- TCP/UDP/ICMP connection requests
- Application connection type, and data volume transferred

69. For each event that is logged, the following information **SHOULD** be logged where available, in order to meet the requirements of the Incident Detection and Response Policy:

- Event name or description
- Date and time
- Account Id
- Command parameter
- IP source and destination address
- Protocol code or description
- Source and destination port
- Success or failure

Critical Security Configuration

70. Security management processes designed to ensure the integrity of the gateway help to achieve the desired level of protection. Whilst 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 staff responsible for drafting the plans and procedures need to know, or be aware of, the critical configurations. The following issues **SHOULD** be addressed:

a. **System Backup Configuration**. The specific components of the gateway that need to be backed up and how this could be achieved **SHOULD** be detailed. It may be necessary to use specific tools or products for this to occur.

b. **Security Configuration Parameters**. The critical configuration parameters used by the gateway **SHOULD** be specified. Gateway staff are best placed to identify a list of those items that require strict configuration controls, as determined in part by the risk assessment process. As a guide, the list **SHOULD** include:

- Firewall access lists
- Firewall management configuration
- Encrypted modem configuration, including key management issues
- Web proxy server configuration

Design Documentation

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

a. **Gateway Logical/Infrastructure Diagram**. A diagram showing the components of the gateway in enough detail to support the Concept of Operations document.

b. **Concept of Operations Brief**. An overview document covering the operation of the gateway.

c. **List of Mandatory Requirements**. This component **SHOULD** detail exactly how the mandatory requirements have been met. This needs to be specific enough so that there is no doubt that all certification requirements have been met.

d. **Risk Based Requirements**. This **SHOULD** be a map of the prioritised countermeasures, with specific reference to those countermeasures designed to counter specific risks. Evidence **SHOULD** illustrate why the countermeasures are considered effective.

e. **List of Critical Configurations**. These are the list of critical configurations that **SHOULD** be checked or changed on a regular basis, to ensure integrity of the gateway operating environment. It may include firewall configuration, proxy server configuration file, audit file, privileged passwords and parts of the account profiles.

f. **Detailed Configuration Documentation**. This is required as part of the detailed design.

g. **Configuration Management Plan**. This details the responsibilities for approving changes to systems, and the process by which these changes should be approved.

Chapter 4
Gateway Security Management

72. 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.

73. 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.

74. The key objectives that influence the tasks of the security administrators can be broken down into a number of distinct components. These are as follows:

a. Security Administration Tasks

b. Proactive Security Configuration Checks

c. Proactive Security Audit Checks

d. Contingency Plans and Tasks

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

76. DSD **RECOMMENDS** that the plans and procedures drafted be brief and concise. They may be stored on-line in a secure environment, but it is **RECOMMENDED** that operators and administrators utilise hard copies of the procedures to undertake the duties detailed in them. These hard copies **SHOULD** be readily available in event of a system outage or compromise.

Security Administration Tasks

77. The security administrative 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 and in what timeframe. A clear linkage between gateway policies and the plans/procedures **MUST** be clearly evident, as well as demonstrating evidence of implementation. For certification, the following plans and procedures **MUST** be developed:

a. **Accounts Administration Procedure**. The profile of system accounts, staff allowed an account on the system, and how often old accounts are to

be deleted **MUST** be detailed, including an outline of accounts administration record keeping. A system in this case could either be an internal server/application, or a user application such as an authentication server, or even a physical access control system.

b. **Privileged Users Plan**. This plan **MUST** detail privileged accounts that are required, and who (by appointment or staff name) is allowed to hold these privileged profiles. Privileged accounts management **SHOULD** be derived from the outcomes of the Security Policy, including password management procedures. See Part 3, Chapter 6 of ACSI 33 for more details.

c. **Access Control Plan and Procedure**. These documents **SHOULD** specify the key access control requirements for a system, in a way that clearly identifies the users (or groups) and their allocated/allowed resources and include the procedure on how to perform access control changes. A system in this case could either be an internal server or application, or a user application such as a web proxy or mail host. See Part 3, Chapter 6 of ACSI 33 for more details.

d. **Key Management Plan and Procedure (conditional)**. Cryptographic key management is crucial where employed in the security environment. These documents **SHOULD** include how keys are derived, how often they are changed for each system, the staff that are allowed access and actions to be taken in event of compromise or replacement. This document is mandatory only where cryptographic services are employed as part of the gateway. See Part 3, Chapter 8 of ACSI 33 for more details.

e. **Physical Access Plan and Procedure**. The plan **SHOULD** detail who is allowed where, to access what equipment and how this is to be controlled.

f. **Backup, Maintenance and Media Control Plan and Procedure**. This document is driven by the requirements of the gateway policies and the design documentation. It **SHOULD** detail those systems that require backup, where a system could be a server, host or application, and the frequency of backup, storage or tapes/disks and period of storage, media reuse/disposal. The backup plan **SHOULD** include backup or archival of logs or audit trails. See Part 3, Chapters 3 and 4 of ACSI 33 for more details.

g. **User Awareness Plan**. This plan **SHOULD** detail the mechanisms for initiating and maintaining a program so that users are aware of their responsibilities, appropriate activities for use of the services and safe practices for use of the services. See Part 3, Chapter 2 of ACSI 33 for more details.

h. **Change Management Plan and Procedure**. These documents **SHOULD** detail the process by which a change is initiated and approved, and the notification mechanisms for stakeholders. Categories of changes need to be identified and those that require a review of the risk assessment noted.

Proactive Security Checking Tasks

78. Proactive security checking is often an overlooked component of the overall security strategy of a system, yet it is the only one that will provide a degree of assurance that the security configuration integrity is intact. These series of tasks **MUST** detail those responsible for checking the gateway system, the components that will be checked and by what means (ie; whether tools are required), how often these checks are to be undertaken, and the authority that is to receive the reports. It is important that the configuration items that require checking and the regularity of checking be derived from the "Critical Configuration List" and the relevant Security Policy.

79. For certification, a clear linkage between gateway policies and the plans/procedures **MUST** be clearly evident, as well as demonstrated evidence of implementation.

80. 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. Plans and procedures **MUST** include:

a. **Firewall Configuration Checking Plan and Procedure**. The plan **SHOULD** clearly detail those 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, the appointment(s) responsible for checking, and who should receive the reports. The procedure **SHOULD** state how the reporting is to be undertaken.

b. **Proxy Server Configuration Checking Plan and Procedure (optional)**. Proxy server configurations are almost always critical to the information passed over the DMZ. The plan **SHOULD** clearly detail those items that need to be checked, what tool will be used to check them, how often this will be undertaken, the appointment(s) responsible for checking, and who should receive the reports. The procedure **SHOULD** state how this is to be undertaken.

c. **Crypto Configuration Checking Plan and Procedure (conditional)**. This document includes cryptographic information associated with remote management, Virtual Private Networks (VPNs), Public Key Infrastructures (PKIs), link encryptors, smartcards or cryptographic tokens, etc. The plan **SHOULD** clearly detail those items that need to be checked, what tool will be used to check them, how often this will be undertaken, the appointment(s) responsible for checking, and who should receive the reports. The procedure **SHOULD** state how this is to be undertaken. This document is conditional on whether these cryptographic systems are employed as part of the gateway.

d. **Alarm and Access Control Plan and Procedures (conditional)**. This document is conditional on whether there is an electronic or semiautomatic

physical entry access control, or an alarm or physical detection system. The plan **SHOULD** clearly detail those items that need to be checked, what tool will be used to check them, how often this will be undertaken, the appointment(s) responsible for checking, and who should receive the reports.

Proactive Security Audit Checks

81. Proactive security audit will alert the security administrators to an increased level of threat against either 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. These series of tasks **MUST** detail those responsible for checking the audit trails, the specific objectives of the checking, 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. It is important that the information required for these tasks be derived from the outcomes of the Gateway Design and the relevant Security Policy.

82. For certification, a clear linkage between gateway policies and the plans/procedures **MUST** be clearly evident, as well as demonstrated evidence of implementation.

83. 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. Plans and procedures **MUST** include:

a. **Real Time Reporting Plan and Procedure**. This document **MUST** be based on the "Incident Detection and Response Policy", and the gateway design documentation. The objective is to ensure there is a plan and procedure to alert the security administrators, in real time, of those events that are crucial to the integrity of the gateway.

b. **Off-Line or Analytical Reporting Plan and Procedure**. This document **MUST** be based on the "Incident Detection and Response Policy", and the gateway design documentation. The objective 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. It is expected that this information could be used, in time, to further develop the risk assessment by providing more realistic figures on the actual threat likelihood. DSD and connected customers **MUST** be an information addressee on these reports, for certified systems.

Contingency Plan

84. 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.

Incident Detection and Response Plan and Procedures

85. These could be covered in the Contingency Plan or separately. The Incident Detection and Response Plan and Procedures **MUST** describe the steps to be followed when the proactive security checking tasks and audit tasks identify a security incident.

86. Identified actions (eg. disconnecting the gateway) **SHOULD** map to the incident categories identified in the Incident Detection and Response Policy. Incident investigation, reporting, evidence preservation, media control and recording, and system recovery procedures **SHOULD** to be outlined in relation to each category of incident.

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

88. All plans and procedures produced **MUST** be directly related to the outcomes of the gateway policies and therefore derived from the results of the risk assessment.