
# GATEWAY CERTIFICATION GUIDE

## VERSION 2.1

Version 2.1 only differs from version 2.0 in that references to ACSI 33 (April 1998) have been amended so as to refer to the December 2000 version of ACSI 33.

Point of Contact: Advice and Assistance group

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

February 2001

# Table of Contents

# Introduction

1. Commonwealth 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 Branch of the Defence Signals Directorate has identified a continuing need for security perimeter (or gateway) protection. This protection is essential when an agency connects to a public network like the Internet. It may also be required when one agency connects to another because the different business needs of the two agencies will mean they have different, potentially incompatible security needs. 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 or compromise of these systems.

## Purpose and Scope

3. The DSD Gateway Certification Process aims to provide a Commonwealth Agency, or a Service Provider to Commonwealth Agencies with an independent assessment that their Gateway has been configured and managed to industry best practice and that appropriate safeguards are implemented and operating effectively. This assurance will provide clients using the gateway services with a level of trust in the service provided. Certification is a voluntary process and this guide is designed to assist agencies that wish to pursue certification (or to recertify) to prepare for the DSD review.

4. The purpose of this document is to provide agencies seeking DSD certification of their gateway facility with details of the requirements that they must fulfil. It is also intended to serve as a reference detailing the areas of specific concern to DSD staff conducting the certification. This would allow agency or company staff to scope, cost and resource the security requirements in advance of the certification process itself. Notwithstanding the above, this document serves to provide guidance and ideas to those agencies seeking to consider secure gateway design, development or management issues. Accordingly, this document could provide a reference for independent "verification" of any gateway system. In any case, it would provide ideas for those staff seeking to design and manage a secure gateway.

5. Issues associated with aggregated gateway services are generically covered in this document, however this is predominantly a risk factor that needs to be

considered as part of the gateway risk assessment.

# Definitions

6. A **gateway** is a secured connection between an internal network and an external network (such as the Internet), but may include connections to other (non-public) systems. It will usually comprise a number of items of computer equipment including a firewall host, proxy servers, routers, email hosts, etc.

7. 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.

8. A DSD gateway **certification** is granted once a gateway system has been assessed by DSD staff to meet the requirements of this publication. A **provisional gateway certification** may be issued to indicate that full certification can be expected, subject to successful completion of a number of stated provisions. This is discussed further in Chapter 5.

9. A **recertification** is undertaken at least once every 12 months after an initial gateway certification has been awarded by DSD. The conditions for recertification are discussed in Chapter 5.

10. An **entry level certification** will be granted to an agency or company whose gateway system has been assessed by DSD to meet the requirements of this publication, but who has yet to connect any Government customers.

11. A **firewall** is the host within the gateway designed to filter 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.

12. The certification process itself will focus on a number of issues, specifically:

A review of the gateway risk assessment. A review of the gateway security policies. A review of the gateway design. A snapshot of the gateway installation and configuration. A review of the gateway security management plans and procedures.

13. The certification process will not be limited to the above issues. Many gateways are operating as complex environments and the function of gateways has expanded from traditional security functions to provision of services eg. E-business, information services, virtual private networks. Under the certification system 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.

14. Agencies and companies involved in the design or management of gateways are encouraged to contact DSD with any comments related to this publication.

# References

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

i. Protective Security Manual.

ii. DSD document "Security Guidelines for Australian Government IT Systems" (ACSI 33).

iii. DSD document "Gateway Accreditation Guide".

iv. DSD document "Firewall Requirements".

v. Australian Standards AS/NZ 4360:1999.

16. This version of the "Gateway Certification Guide" replaces items iii and iv above.

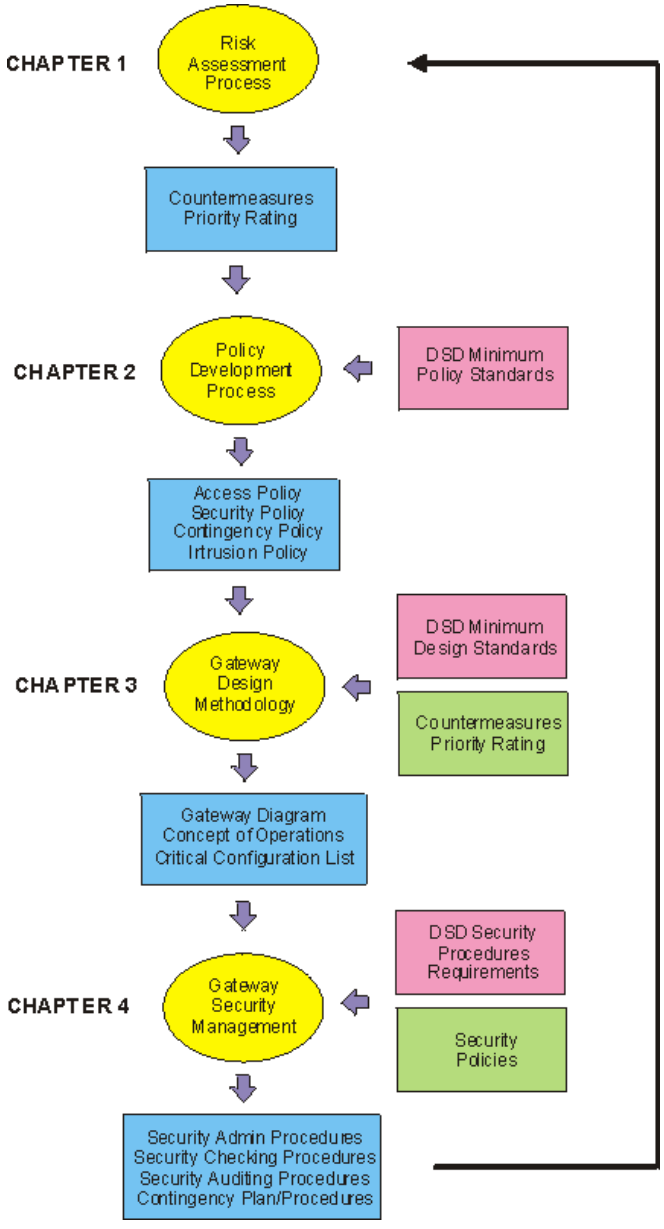
# Gateway Development Process

17. The chapters in this manual are designed with Figure 1 in mind. Chapter 1 covers the security risk assessment methodology that could be used for determining risks to a gateway environment. Chapter 2 covers the policy development process, noting the linkage between it and the risk assessment process. The technical design is driven directly by the policy, rather than the risk assessment. Gateway design is covered in Chapter 3. DSD Certification requirements come into play where minimum policy standards are mandated, for systems that require certification.

18. The development of a security management regime is discussed in Chapter 4. The business processes used to provide the required level of security assurance to the customers and managers of the gateway environment are

discussed in detail, and should be derived from the policy and design documentation. The business processes should therefore be indirectly driven by the risk assessment. Chapter 5 details the DSD requirements for certification of a gateway system.

**Figure 1:** Gateway Design Process



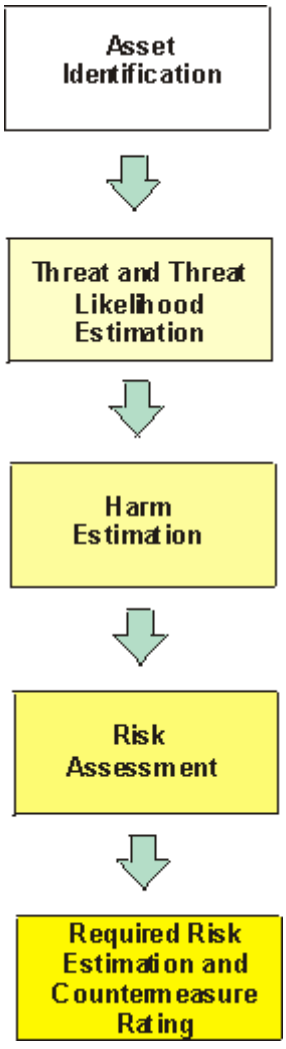
# Chapter 1

# Security Risk Assessment

100. As a security tool, risk assessment methodology aims to provide a degree of assurance that the resource cost of security countermeasures used to counter specified threats is commensurate with the risks. The risk assessment methodology used in this manual has been adapted from the Australian Standard AS/NZ 4360:1999 titled "Risk Management", and other sources.

101. A gateway is a risk mitigation strategy. The countermeasures that are employed by the gateway including use of trusted products, configuration, design, ongoing monitoring and auditing, are all designed to minimise the risk. The risk assessment process involves identifying key gateway assets, identifying and quantifying the threat likelihood (wherever possible) against each asset, determining the harm profile against each threat, and calculating the current risk for each asset. Determining an acceptable level of risk for each asset/threat pair, and the priority of the associated countermeasure (in broad terms) is the final step in the process. This process is shown in Figure 1.1. The outcomes of the risk assessment are used to provide ***guidance*** on the assets that are most at risk.

**Figure 1.1:** Security Risk Assessment Methodology




102. Risk assessment can be applied to a myriad of conceivable assets and processes within any gateway environment. However, the aim of the assessment is to limit the scope, to the granularity of those asset/threat pairs that are appropriate for providing guidance to the next steps in the gateway design, namely the policy development and the technical design. An example of the level of granularity that would be required is given in the example risk assessment in Annex A. The level of granularity is left to the those responsible for drafting a risk assessment, who should be mindful of the negative impact of a lengthy, confusing risk assessment guide.

103. The risk assessment provides guidance on the level of risk to be expected in a contemporary gateway environment, **before** the gateway has been designed or the policy developed. The risk assessment should therefore be

developed so as to guide the design and policy development processes. By developing the security risk assessment for a gateway **without** the countermeasures in

place it is possible to revisit the assessment at a later stage, with a view to determining the appropriateness of those countermeasures in a changing or dynamic security risk environment.

# Asset Identification

104. This component provides guidance on those gateway assets that could be broadly considered in the context of a risk assessment. An "asset" can be a tangible quantity (such as hardware item), a grade or level of service, staff, or information. It is important that the key assets for a gateway be identified and the assessment encompass all relevant risks and therefore countermeasures, so that the policy and design development can be undertaken in an informed manner. The assets could be briefly described as "what needs to be protected", but they also need to be attributed a value so that the harm can be identified at a later stage in the process. It is also essential that the owners/persons responsible for the asset are identified.

105. As a guide, the following assets could be defined for a secure gateway environment:

***Integrity of gateway security functions***. This asset is defined so as to recognise that maintaining a secure configuration is a critical success factor for design of a gateway. For example, a "small" change in the firewall access list could have a severe impact on which services and resources can be accessed on internal networks by external, unauthorised staff. The definition should therefore be viewed as a "grade of service" that would be expected by customers or users of the gateway. It could be broken down into more manageable components, if required.

***Availability of gateway resources and services***. This asset will likely be the most critical to customers and users of the gateway. It may be broken down into key services to better assist the gateway designers. For example, resilience or availability of email, web and ftp services could be considered separately.

***Operating environment free from viruses or maleficent trojan code***. This would include obvious infections via email attachments or ftp (consequently applies to all traffic transiting the gateway), but may also include Active-X viruses or Java applet trojans. Generic or specifically targetted trojans could also be considered, and this asset could be broken down to treat each service separately.

***No accidental leakage of classified or sensitive information***. This is a gateway "feature" that could be included to provide guidance to the policy

and design development process. It is obviously applicable to applications such as email and web services.

***Secure support environment***. A general term that includes the actual building(s) and all supporting facilities and equipment. For example, a building asset includes the uninterruptible power supplies, air conditioning equipment, electrical distribution boards, security access control system, alarms, on-site guards, etc.

***Equipment***. Includes IT related equipment from PCs to mainframe, PABX systems, photocopiers and printers. All the smaller office items can also be included in this category

106. It is important that those staff member(s) undertaking the risk assessment determine the appropriate level of granularity for asset identification process. Annex A provides some examples on the level of asset identification granularity, based on the categories listed above. This could be used as a guide in developing a security risk assessment.

# Threats and Threat Likelihood Estimation

107. Identifying the nature of individual threats, their source and probability of occurrence is the next step in the risk analysis process. There could be multiple threats associated with one asset, and this should be reflected in the risk assessment process. It is counterproductive to detail all conceivable threats associated with an asset (eg; there is a threat that the gateway could be destroyed by a falling building). Only those threats that could reasonably be expected to occur, or those threats, that if realised, will result in high or extreme harm, should be considered.

108. Information on the probability of external threats can be derived in quantitative form from police force reports, computer security surveys and bulletins, results of audit analysis or actuarial studies. The likelihood of internal threats may not be so readily ascertained. They can be estimated using previous experience, generic statistical information or a combination of the above. DSD may be consulted for advice on the threat or threat likelihood.

109. Some threats can be increased by inadequate security procedures, introducing a "feedback loop" into the risk assessment equation. For example, if no security countermeasures are provided for building access control, this weakness may eventually be exploited, and the lack of security controls actually contributes to the increased threat likelihood. The security risk assessment methodology presented in this chapter and has been adapted so that these "feedback loops" are not relevant to the estimation of risk.

110. The source of the threat may be used in determining its probability. The threat probability is a measure of the likelihood of the threat being realised. Risk analysis methodologies include determining the threat by qualitative, semi-

quantitative or fully quantitative methods. It is important that the best educated, informed estimate be used to provide realistic guidance for the risk assessment. This guide uses a semi-quantitative approach. The scale below in Table 1 could be used as a basis for categorising the threat probability or likelihood:

| | |
|---|---|
| ***Negligible*** | Unlikely to occur; |
| ***Very Low*** | Likely to occur two/three times every five years; |
| ***Low*** | Likely to occur once every year or less; |
| ***Medium*** | Likely to occur once every six months or less; |
| ***High*** | Likely to occur once per month or less; |
| ***Very High*** | Likely to occur multiple times per month or less; |
| ***Extreme*** | Likely to occur multiple times per day. |

**Table 1:** Threat Likelihood Rating

111. In drafting the risk assessment, it is good practice to document or reference the figures derived for the threat likelihood. Details of any research activity undertaken to better estimate the threat likelihood should be clearly referenced in the assessment, to provide accountability in the original draft, and continuity when reviewing the assessment at a later stage. Previous history on the assessed threat, such as audit trail analysis reports, should also be clearly referenced.

# Harm Estimation

112. The harm caused to the gateway services or resources, as a result of the loss or compromise of an asset will vary with the nature of the asset. It should be clearly noted that the harm *is not* related to the threat likelihood. For example, the threat likelihood of the loss of a proxy server due to an unstable operating system may be "high", but the harm may be "minor" if the proxy server supporting the service or resource is not viewed by the data owner or management as critical. Alternatively, the likelihood of accidental misconfiguration of the firewall may be "very low", but its impact or harm could be "serious" to the security integrity of the gateway.

113. Table 2 is a guide to the harm definitions that could be used in developing a risk assessment. The definitions used below may be changed, if necessary. It is

important to remember that the words used to describe the harm is not the critical component, rather how the terms have been defined.

| | |
|---|---|
| **Insignificant** | Will have almost no impact if threat is realised. |
| **Minor** | Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure gateway. |
| **Significant** | Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or agencies. Will require some expenditure of resources to repair. |
| **Damaging** | May cause damage to the reputation of the gateway management, and/or notable loss of confidence in the gateway resources or services. Will require expenditure of significant resources to repair. |
| **Serious** | May cause extended gateway outage, and/or loss of connected customers or business confidence. May result in compromise of large amounts of Government information or services. |
| **Grave** | May cause gateway to be permanently closed, and/or be subsumed by another secure gateway environment, May result in complete compromise of Government agencies. |

**Table 2:** Harm Estimation Rating

114. Even though a threat likelihood may be assessed as "very low", if the harm the threat may cause is "serious" or "grave", then the overall risk can be significant. While the threats to an asset can be quantified or qualified by security specialists, the harm to an asset will always be an executive, asset owner or asset manager determination. This is the key to conducting a successful risk analysis; clear involvement of the executive or management of the relevant agency(ies).

# Risk Assessment

115. Mathematically, risk can be expressed as

***threat likelihood x harm = risk***

116. While this equation lends itself to production of a statistical or quantitative analysis, it indicates the two key factors that need to be considered for the analysis of risk. A general semi-quantitative analysis will greatly promote a security policy and technical design criteria that focuses limited resources on those (relatively) high security risks. The outcome of the risk assessment is an expression of whether the residual risk is acceptable. Security specialists and other managers can use this information to determine the general security countermeasures (if any) that may be required to reduce the risk to an acceptable level, and the order in which they should prioritise those countermeasures.

117. In the absence of a detailed statistical method, the risk assessment example provided in the annexes to this chapter should be interpreted as guidance on those high security risks faced by the gateway security management. In the future, as more detailed statistical data becomes available, the threat likelihood and therefore the risk assessment should reflect the actual risk more accurately. This could be achieved by conducting sensible auditing of the real-life threats and their likelihoods.

118. Using the definitions of *threat likelihood* (Table 1) and *harm* (Table 2) defined earlier in this chapter, the data shown in Table 3 could be used to produce the resultant risk:

| | | Harm | | | | | |
|---|---|---|---|---|---|---|---|
| | | **Insignificant** | **Minor** | **Significant** | **Damaging** | **Serious** | **Grave** |
| **Threat** | **Negligible** | Nil | Nil | Nil | Nil | Nil | Nil |
| | **Very Low** | Nil | Low | Low | Low | Medium | Medium |
| | **Low** | Nil | Low | Medium | Medium | High | High |
| | **Medium** | Nil | Low | Medium | High | High | Critical |
| | **High** | Nil | Medium | High | High | Critical | Extreme |
| | **Very High** | Nil | Medium | High | Critical | Extreme | Extreme |
| | **Extreme** | Nil | Medium | High | Critical | Extreme | Extreme |

**Table 3:** Resultant Risk

119. Table 3 shows the risk mapping, using the threat likelihood and the harm ratings. The outcome resultant risk provides a grading as to the expected risk *without* any applied countermeasures. The final step in the risk assessment process uses this information to provide guidance to the policy and design development staff on which countermeasures should be prioritised.

# Required Risk and Countermeasure Rating

120. The required risk should be the desired "risk level", as required by the management authority of the gateway. One method that could be used to derive the required risk, is to use the following statement:

***"The Required Risk is the risk level that management are prepared to accept."***

This is best illustrated using the example Risk Assessment in Annex A.

> Row 3 in the table details two threats to the same asset. The first threat (IP Denial of Service) states that the threat likelihood is "Extreme" (Table 1 - may happen a number of times per day) and the harm is "Damaging" as per Table 2.
> Using Table 3, the resultant risk is therefore "Critical". However, management require that the threat likelihood be mitigated so that it should only occur once every two/three years or less (threat likelihood = very low).
> Again, using the mapping in Table 3, the "Required Risk" (Column 6) then becomes "Low".

Another example.

> Row 4 (Integrity of Firewall access rules) produces a resultant risk (Column 5) of High.
> Management have decided that this level of risk be mitigated to Nil (Column 6), and will therefore accept a situation where the firewall access rules are *unlikely* to be inadvertently changed.

121. The final part of the assessment is the countermeasure priority rating. The countermeasure rating is the difference between the required risk and the resultant risk, and is used to provide guidance as to the importance that should be placed on broad security countermeasures. The following table is used to calculate the countermeasure rating (as shown in Column 7 in the example):

**Risk Rating:**

| | |
|---|---|
| Nil | 0 |
| Low | 1 |
| Medium | 2 |
| High | 3 |
| Critical | 4 |
| Extreme | 5 |

122. Column 7 in the example is simply the difference between the resultant risk and the required risk (or Column 6 and Column 5 in the example), expressed as a number. The critical outcome is the resultant prioritised countermeasures, relative to one another (Column 7 in the example).

123. The priority of the countermeasures should be reflected in the policy and

plan documents developed in the following chapters. These may relate to:

- addition of security measures
- reduction of inappropriate security measures
- risk avoidance through change of service and system specifications
- acceptance of residual risk
- minimisation of harm through response mechanisms.

# Chapter 2

# Gateway Policy

200. The Gateway Policy needs to describe the philosophy by which the gateway is managed. DSD staff 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.

201. A number of gateway policy documents are required for certification. They are discussed in this chapter. Unlike previous versions of this and other documents, DSD will no longer furnish "template" security policies to agencies since this approach has not proven to be useful in the past. Agencies are encouraged to draft the policy in their own terms and definitions, and in a manner that would be best accepted by their relevant agency management and staff.

202. The Gateway Policy has a number of subsets, namely the Access Policy, Security Policy, Contingency Policy, Incident Detection and Response, and Configuration Control. As a guide, the total policy statements should be no more than 10 – 15 pages, clearly detailing the key policy objectives and responsibilities. Details on how the gateway is to be managed, and how policy issues are implemented are to be addressed in plans and procedures documents (discussed in Chapter 4), and not in the policy documents.

## Risk Assessment Methodology and DSD Certification Standards

203. In drafting this guide, maximum flexibility in designing a gateway has been afforded the designers of gateway policies and infrastructure, in adopting risk management methodology to tackle the security problems. However, DSD expects minimum standards in some areas of the gateway policy. These minimum standards have been annotated in this chapter in **green**, so their intention and application is clear. In addition, these minimum standards are also listed at the end of this chapter.

## Access Policy

204. The Access Policy should by default deny all services unless expressly permitted. This applies to both internally or externally generated connections. This policy should also detail which services are allowed, both for incoming and outgoing connections. The results of the risk assessment (see Chapter 1) should be used as the basis for detailing those services that will be allowed. However, customer security requirements 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) should be used to provide an

access policy that details:

vi. Those services available to all internally connected clients.

vii. Those services available to all external users.

viii. 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(ies).

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

x. Access between internal 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.

205. 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, whether it be via a legally binding MOU, or formal correspondence via an agent on behalf of the agency head. **For DSD certified systems, the access policy needs to be derived from the results of the risk assessment and the customer requirements (if any), and this linkage should be clearly detailed in the policy**.

## Security Policy

206. The Security Policy needs to detail the management of various security aspects of the gateway. The results of the risk assessment should be 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. **For DSD certified systems, a clear link between the risk assessment and the security policy needs to be established, so that the security policy objectives and their associated countermeasures are appropriate for the level of identified risk**.

207. The security policy can be divided into the following components:

i. *Administrative Security*. Detail the maximum classification of data that will be handled, or *could* be accessed by staff in the gateway environment. This section should also 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. **For DSD certified systems, only those systems handling HIGHLY PROTECTED or below, or RESTRICTED or below will be certified by DSD**.

ii. *Personnel Security.* 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 needs to also be included. This component should also include legal conditions obligated on employees, as well as contractors.

iii. *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. **For DSD certification, physical security of the all gateway premises must meet the standards detailed in Handbook 14 of ACSI 33 or where necessary the standards detailed in the Handbook 14 Supplement**.

iv. *Communications and Key Management Security*. This section should 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 needs to be handled in the same manner as privileged accounts. **For DSD certification, cryptographic key management must be in accordance with either the ACSI 53 and/or the ACSI 57, depending on whether low grade or high grade encryption services are being used**. The ACSI series of documents are available by contacting DSD staff.

v. *Equipment Maintenance and Disposal*. This section should cover 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.

vi. *Normal and Privileged Access to Systems*. Management must detail those staff or appointments that are allowed unsupervised access to the systems, and which particular staff or appointments will be granted superuser or privileged access to specified systems. Privileged access is defined as access which may give the user the ability to change key system configurations, or have access to audit or related information, or have access to data streams, files and accounts owned by other users.

vii. *Media Security.* An important component of the overall security policy is that associated with handling and control of storage media. Included are requirements for accountability of media within the gateway environment.

viii. *Configuration and Change Control.* This should detail the responsibilities for approving changes to systems, and the process by which these changes should be approved. Stakeholders in the change process should be defined. The gateway design documents (discussed in

Chapter 3) should detail the critical components of the gateway. This policy item should therefore not be concerned with identifying at what level of detail a configuration change should be identified, but rather the process by which these changes should be efficiently and effectively handled. Reference should be made to the design documentation. Given that the risk assessment encompasses all current clients and services, it is beholden upon all clients to accept and exercise their stakeholder rights or obligations in any actions that may affect the security of the gateway.

ix. *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.

x. *Agency and Service Provider Responsibilities (external service provider only).* Where gateway services are provided by an external service provider, the attribution of liability and acceptance of residual risk needs to be documented and understood. All clients should satisfy themselves that the risk mitigation strategy and security policy are acceptable throughout the period of any contract with the service provider.

## Contingency Policy

208. The contingency policy must detail the critical management objectives for a contingency plan. **For DSD certified systems, a clear link between the risk assessment and the contingency policy needs to be established, so that the contingency policy objectives are appropriate to the level of identified risk.** The policy should deal with the following issues:

i. 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.

ii. Definitions of contingency outages, and the appointment responsible for declaration of each grade of a contingency outage.

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

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

v. On-line redundancy and off-line redundancy.

209. The results of the risk assessment should be used to provide guidance for required recovery times. In particular, specific attention should be paid to priority of systems and realistic recovery times, allowing maximum flexibility for the management team in event of an outage.

## Incident Detection and Response Policy

210. This section could have been covered either by the Security or Contingency Policy. However, it should be addressed separately to reflect its importance in the

management of a secure gateway.

211. Clear definitions on the types of incidents that ***are likely*** to be encountered need to be detailed, so that a documented plan can be derived to alert management to the expected response. As a guide, the types of incidents could be categorised as follows:

i. **Category 1: Attempts to gain technical information on the Gateway.**

Effect: Possible Information Security Incident; No effect on system operations
This would include the use of port /address scans, probes and finger commands. Legitimate methods of seeking information, such as DNS queries, Web page requests, etc should NOT be included as attempts to gain information. This grade would (for example) include an attempt to gain access to the TELNET service. However, repeated attempts may be listed under the following grade.

ii. **Category 2: Unsuccessful attempts to subvert the Gateway.**

Effect: No effect on systems operations
This includes all obvious attempts to interfere with the confidentiality, integrity or availability of the Gateway. This would include attempted Trojan attacks, unsuccessful denial of service attacks, and unsuccessful authentication attacks (subject to an appropriate and agreed threshold). It would also include attempts to gain information or subvert staff via social engineering, as well as virus attacks that have been trapped by the virus scanning software.

iii. **Category 3: Successful attempts to subvert the Gateway.**

Effect: Minor or Moderate effect on systems operations
This includes all attacks that have successfully interfered with the confidentiality, integrity or availability of the Gateway. Successful attacks, such as Web Server attacks, mail host attacks, denial of service attacks etc are therefore included in this grade. Virus attacks that have caused an outage or system problem and not been detected by the scanning software should also be categorised as a Category 3 incident. This category would include DNS mirroring or related spoofing attacks. It will be of interest to DSD certification staff to assess how a successful intrusion ***could*** be detected.

iv. **Category 4: Major successful attempts to subvert the Gateway**

Effect: Major damage or effect on systems operations
This includes any situation in excess of the above examples or any situation where a high level of crisis management is necessary.

212. The categories of incidents discussed above 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. Based on the above, this policy component should cover the following issues:

v. Detail security objectives for real-time reporting (this must be specific, and based on the incident grading definitions). These objectives should be realistic and achievable. It should include what category of incident should be reported on a real-time basis, who should receive the report and whether the reports need to be formally acknowledged or reported to higher levels. **For DSD certified systems, DSD must be notified as soon as practicable of all Category 3 or higher incidents.** This should be done by the **ISIDRAS** reporting methodology.

vi. Detail the security objectives for off-line or analytical reporting (this must be specific, and based on the incident category definitions). This objective should define the regularity for producing analytical reports, what category of incident should be reported and who should receive the reports. **For DSD certified systems, DSD and connected gateway customers must be an information addressee on off-line, analytical reports. This requirement is detailed in later chapters**.

vii. Detail the policy on archiving of logs. Include how often the logs should be archived, how long they should be stored, whether they should be backed up, and whether the backups should be stored off-site. **For DSD certified systems, agencies must keep archives of logs for no less than 12 months, and these archives should be stored securely off-site**.

Detail the authority(s) responsible for initiating a formal (administrative) investigation and police investigation of an incident. Note that this may overlap with some of the provisions of a Contingency Policy. Outline the criteria by which the responsible authority(s) would initiate a formal or police investigation of an incident. This section should also detail which agencies or authorities should be informed in event of an investigation being undertaken. **For certified systems, DSD must be an information addressee on incidents that require formal investigative action**.

viii. Detail the response that is to be followed given expected, predicted or possible incidents.

## Minimum Policy Standards Required For DSD Certification

213. This chapter contains a number of policy objectives that are viewed as mandatory for those gateways that will require DSD certification. These objectives are part of the discussions in the chapter, but are summarised as follows:

i. The access policy needs to be derived from the results of the risk assessment and the customer requirements (if any), and this linkage should be clearly detailed in the policy.

ii. A clear link between the risk assessment and the security policy needs to be established, so that the security policy objectives and their associated countermeasures are appropriate to the level of identified risk.

iii. Physical security of all the gateway premises must meet the standards detailed in Handbook 14 of ACSI 33 or where necessary the standards detailed in the Handbook 14 Supplement.

iv. Cryptographic key management must be in accordance with either the ACSI 53 and/or the ACSI 57, depending on whether low grade or high grade encryption services are being used.

v. A clear link between the risk assessment and the contingency policy needs to be established, so that the contingency policy objectives are appropriate to the level of identified risk.

vi. DSD must be notified as soon as practicable of all Grade 3 or equivalent incidents.

vii. DSD and connected gateway customers must be an information addressee on off-line, analytical reports.

viii. Agencies must keep archives of logs for no less than 12 months,

and these archives should be stored securely off-site.

ix. DSD must be an information addressee on incidents that require formal investigative action.

x. Only those systems handling HIGHLY PROTECTED or below, or RESTRICTED or below will be certified by DSD.

# Chapter 3
# Gateway Design

300. 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.

301. As discussed previously, the gateway design concepts described in this chapter are recommended for protection of networks processing a maximum of HIGHLY PROTECTED or lower rating; or networks processing a maximum of Nationally Classified RESTRICTED or lower material; from public networks such as the Internet. Protection of networks processing higher classifications by a gateway connecting to public networks or ratings is not recommended, and will not be certified by DSD.

302. This chapter is essentially broken down into two components. The first component details the design criteria that is mandatory, if seeking DSD certification. The second component discusses the design criteria that is subject to a risk assessment. Where possible, maximum flexibility has been afforded the designer and the mandatory requirements have been kept to a minimum.

303. The following diagrams depicting gateway components and network separations are not intended to be prescriptive architectures. As stated previously the gateway architect should use risk based design criteria in order to develop the appropriate gateway architecture to suit the environment. Mandatory requirements should be incorporated into the design.

## Gateway Major Components

304. Figure 3.1 below illustrates the gateway major components. The External/Public network is usually the Internet, but can be any lower classified network. The Demilitarized Zone or 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. The application proxies (if any) offered as part of the commercial firewall may be used subject to those components being evaluated by DSD. The central component of the gateway is the firewall, and it is for this reason that the firewall be evaluated and configured to meet the DSD E3 evaluation standard (as discussed later).

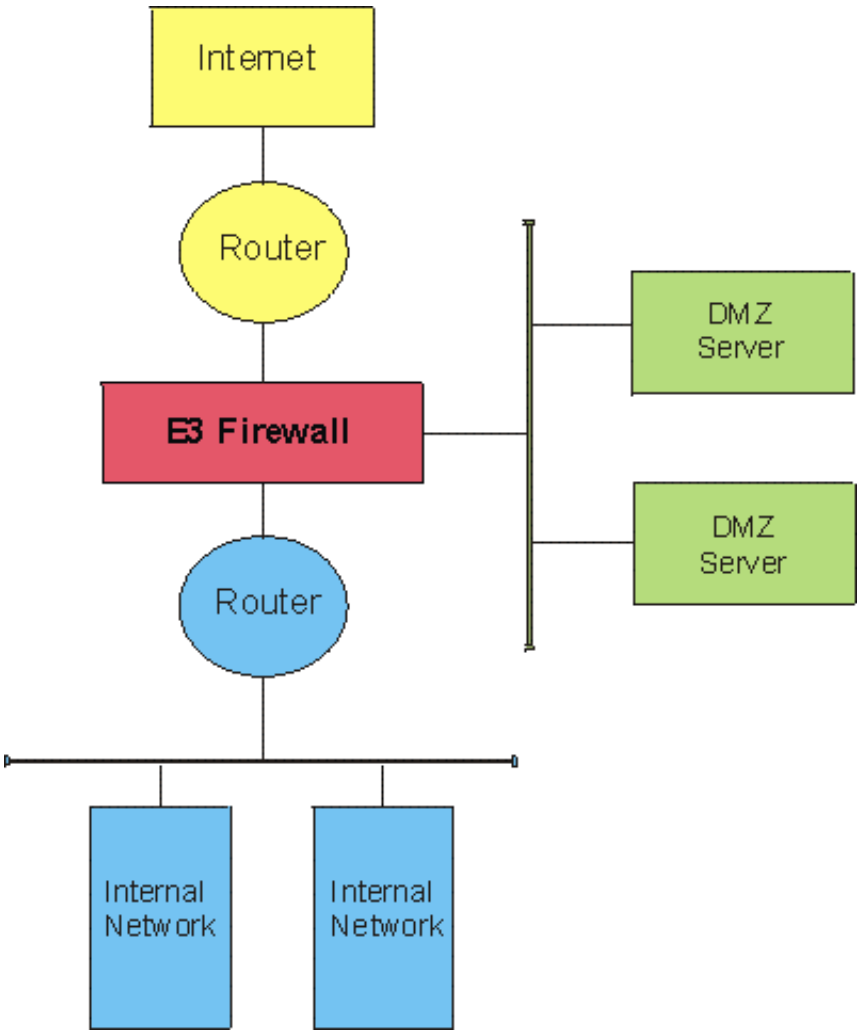



**Figure 3.1**: Major Components, Single User Gateway

305. Designers should note that not all firewalls which support multiple ports provide trusted separation between those ports. This would be required if the firewall was being used to service multiple customers. Designers should ensure, in consultation with DSD, that the functionality required to provide port 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. The requirement for multiple DMZs is discussed later in the chapter. It should be noted from Figure 3.2 that multiple firewalls are not always required to service multiple customers.

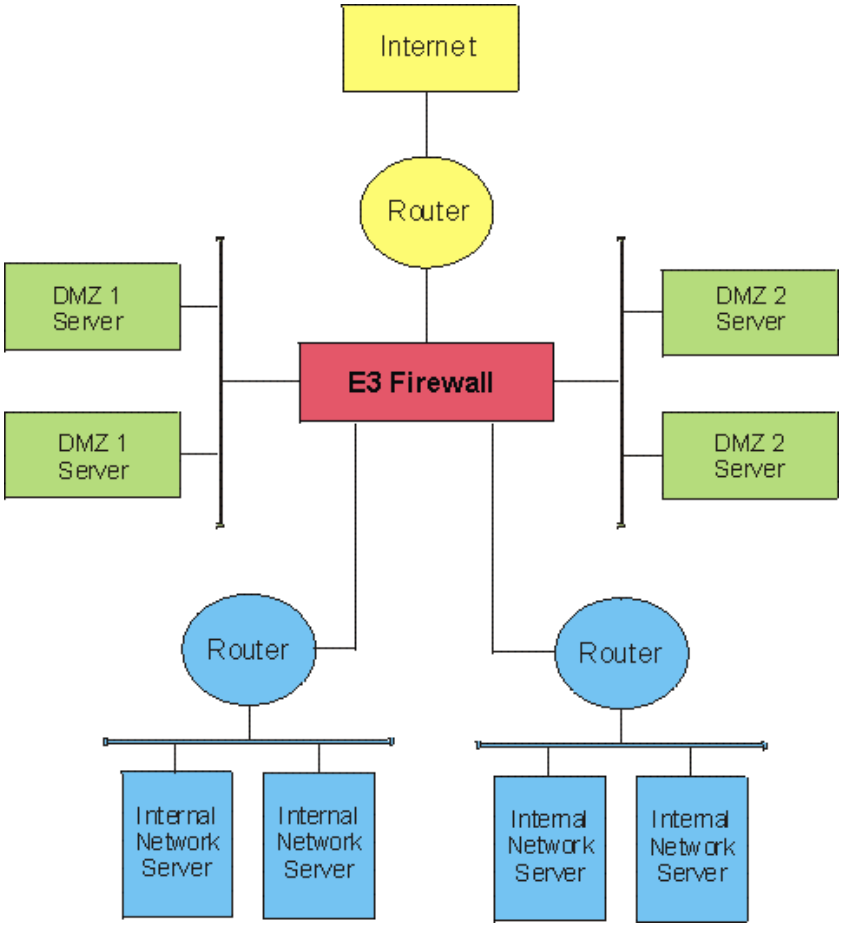



**Figure 3.2**: Major Components, Multiple User Gateway

306. In the event that the firewall of choice does not have enough port connections, another (evaluated) firewall may be chained to provide security services to other internal networks. The DMZ servers may contain a number of hosts and could be implemented by establishing a LAN with a number of servers. Positioning of dial-in services, as well as other services provided by the gateway, are subject to risk based design criteria which should examine what data classification resides on these servers, what data is accessible from 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

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

308. Incoming and outgoing services (to either the internal network(s) or the DMZ) must be denied by default. This is usually a feature of most commercially

available firewalls, although some configuration may be involved. In any case, this is the default policy that is required. Designers should note that the default policy is also required for the proxy or other servers on the DMZ, since this will minimise exposure to those servers and therefore services.

309. 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. The Access Policy (described in Chapter 2 - Access Policy) is to be used to provide direction in this manner.

310. All IP based network communications 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 in this criteria 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 which potentially bypass gateway safeguards.

311. In 1998, the Australian Government issued a Cabinet Directive which imposed a requirement on Commonwealth agencies acquiring new encryption products to purchase only from a list of those products approved by DSD and to use the facilities incorporated in products to prevent the loss of Government information which has been encrypted. All implementations of cryptographic services in the gateway, including those for confidentiality, authentication, non-repudiation or data integrity should be included within the DSD approval process. 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.

312. When selecting any products from the DSD Evaluated Products List, Government Departments are recommended to consult with DSD regarding their requirements and the use of the listed products. ACSI 33 defines the minimum formal assurance levels recommended for a firewall or security filter used to connect networks. The assurance level is just one of the issues which should be considered when selecting components to form a security architecture. Governments Departments, in conjunction with DSD, should ensure that products selected from the EPL have the necessary assurance level for the intended use, as well as the appropriate evaluated functionality to provide the required security services.

313. The Protective Security Manual (PSM) mandates the use of a DSD approved firewall for connecting any agency network to an external network. A DSD approved firewall consists of an E3 evaluated firewall whose installation is certified by DSD. Designers should be aware that whilst a particular commercial firewall may be evaluated to E3, some components of the firewall may not be approved. Accordingly, designers should consult DSD to obtain a copy of the

Certification Report for the particular firewall which will detail the scope of the evaluated version and recommendations regarding its use in the Australian Government environment. Designers should consult with DSD before selecting a firewall which is listed on DSD's Evaluated Products List but is only "in evaluation". Designers should also be mindful of the statement about multiport firewalls in paragraph 304. While E3 is the recommended assurance level for connecting to public networks, E1 may be acceptable for inter-government agency connections or connections from IN-CONFIDENCE networks to public networks, however, some consideration should be given to application level functions required as part of the risk assessment.

314. All communication links between the internal network components and the firewall, where the communications path is not physically controlled by agency and contractor staff identified in paragraph 207vi (eg. a connection via a telecommunications carrier to a remote site providing gateway services) must be encrypted by a DSD approved method. Firewall management shall 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. As discussed above, the remote management feature, if available, must have been approved by DSD as part of the E3 evaluation.

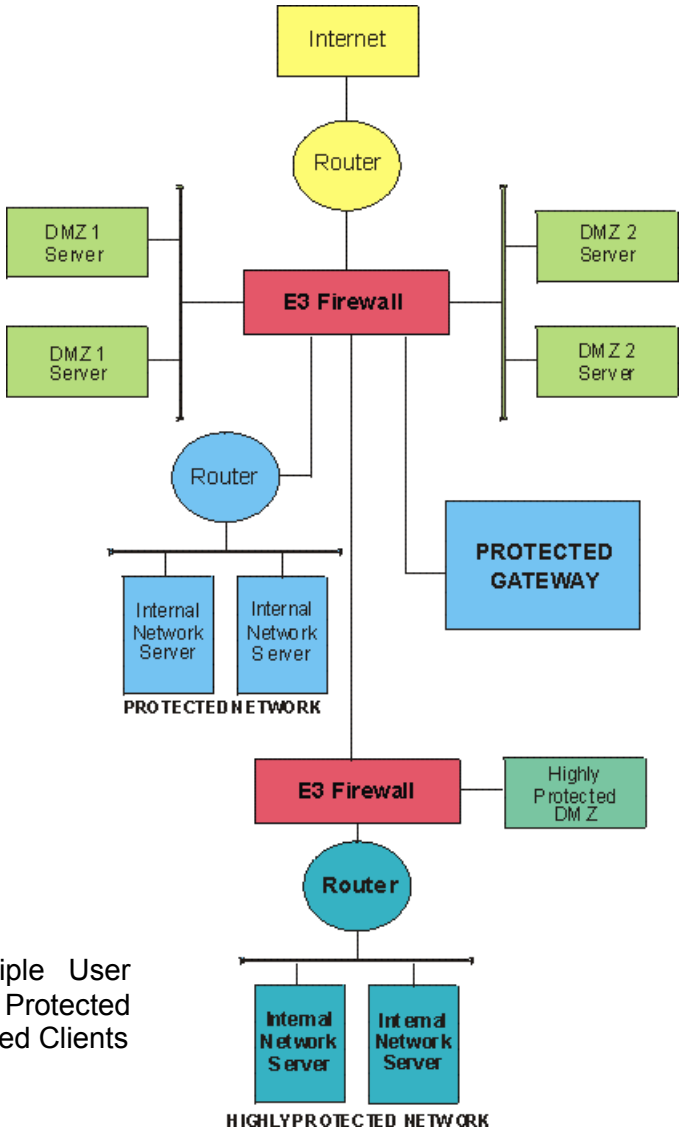



**Figure 3.3**: Multiple User Gateway, Serving Protected and Highly Protected Clients

315. No services are to 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, must be proxied through the DMZ servers.

316. The internal and external border router(s) (refer Figure 3.1 or 3.2) should be configured for access control only where absolutely necessary. This is to allow as many service/connection requests to be passed to the firewall, so that it may have the capability to log all successful and unsuccessful attempts at connection. If appropriate some firewall access controls could be copied to border routers to filter low category attacks, however border routers cannot be relied upon for access control.

317. Figure 3.3 shows the configuration for HIGHLY PROTECTED clients. For those gateways offering services to HIGHLY PROTECTED clients, the second firewall shown in the figure must be from a different manufacturer than the primary firewall.

## Risk Based Security Design Criteria

318. This section details those gateway design design aspects that should be based on the outcomes of the risk assessment. As discussed in later sections, it is recommended that a clear linkage between the results of the risk assessment Countermeasure Priority Rating – Annex A to Chapter 1) and the actual designed countermeasures be established.

319. Security services available on gateway servers will be protocol specific, and are to be determined by a risk assessment. Subject to the outcome of a risk assessment, as an example, the following common services may be required to be protected by the following application level security objectives:

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

ii. Email. Virus detection software should be executed on all incoming and outgoing mail. Only those email messages that have a valid UNCLASSIFIED label on the first line of text (for example) will be forwarded to the outside network.

iii. Web. Java applets to be blocked. Web pages that are copied from the internal network to the DMZ should be pushed from the internal network, and not pulled from the DMZ.

320. Measures designed to mitigate risks to availability will greatly depend on the results of the risk assessment. However, it would be prudent to consider some on-line redundancy into the system, as well as a contingency plan to cater for an off-line "cold" site. The outcomes of the Contingency Policy, discussed in Chapter 2 Contingency Policy should be used to drive those issues regarding availability, especially the extent and balance between on-line and off-line redundancy. Consideration also needs to be given to how system backups will be undertaken. The extent of backups will be dependent on the system design, including the redundancy built in to the system. The Security Policy (Chapter 2 - Security Policy) should be used for guidance. Audit log backups should be treated differently due to the evidence/forensic requirements for the data contained in these logs. Archive, storage and management of audit logs should reflect the requirements of the Incident Response Policy/Plan.

321. Auditing or logging services need to 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 also need to be provided to monitor the administration of the gateway. The results of the Incident Detection and Response Policy (detailed in Chapter 2 - Incident Detection and Response Policy) 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 designer should review the information contained in logs and identify critical patterns to form the basis of exception reporting. The manual review of log data over a long period of time, without the use of tools to reduce the information to critical events and analyse patterns, is open to error and can often be overlooked. The best approach employs a combination of manual review and exception reporting.

322. The off-line or analytical reporting may be provided by a commercial or locally designed tool. The level of monitoring designed for the gateway should be such that the following events are recorded, for both successful or unsuccessful attempts. The events have been separated into "Management Events" and "Gateway Network Events", as follows:

323. *Gateway Management Events.*
This includes events that occur on the firewall, DMZ server(s) or other critical components.

xi. Logon and logoffs.

xii. Boot and initialisation.

xiii. Shutdown, and associated details.

xiv. Restart, and associated details.

xv. Changes to the firewall configuration.

xvi. Access/Security Policy exceptions.

xvii. Password changes.

*Gateway Network Events.*
The log containing this information may be either the raw, logging information or the processed outputs. As mentioned previously, the gateway designer should examine how the security auditing objectives can best be achieved. As a guide, the following information may be collected:

i. TCP/UDP/ICMP connection requests.

ii. Application connection type, and bytes transferred.

iii. Policy exceptions.

324. For each event that is logged, the following minimum information may be logged where appropriate, in order to meet the requirements of the Incident Detection and Response Policy:

i. Event name or description.

ii. Date and time.

iii. Account Id.

iv. Command parameters

v. IP source and destination address.

vi. Protocol code or description.

vii. Source and destination port.

viii. Success or failure.

ix. Byte size.

## Critical Security Configuration

325. Unless it is configured and managed correctly, a gateway implementation may not achieve the desired level of protection. Security management processes designed to ensure the security integrity of the gateway are a key feature of maintaining a secure environment. Whilst the proper configuration of the firewall at installation time is important, the business processes used to pinpoint problems, correct errors, detect misconfigurations, detect and 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 (Chapter 4) need to know or be aware of the critical configurations, some of which are discussed below. The following issues should be addressed:

xi. System Backup Configuration. What specific components of the gateway

need to be backed up and how could this be achieved. It may be necessary to used specific tools or products for this to occur.

xii. Key Security Configuration Parameters. The critical configuration parameters used by the gateway should be specified. The gateway designer is 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

326. The design documentation that is recommended, and necessary for DSD certification should be no more than about 10 - 15 pages. It should be broken down into the following components:

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

ii. *Concept of Operations Brief*. A document no greater than 5 pages detailing the operation of the gateway.

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

iv. *Risk Based Requirements*. This should be a map of the prioritised countermeasures (see Chapter 1 Risk Assessment), with specific reference to those countermeasures designed to counter the specific risks. Evidence is required that illustrates why the countermeasures are considered effective.

v. *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 firewall operating environment. It may include firewall configuration, proxy server configuration file, audit file, privileged passwords, parts of the account profiles. The designers should also specify how these configurations/settings can be most efficiently checked on a regular basis.

vi. *Detailed Configuration Documentation*. This is required as part of a detailed design.

# Chapter 4
# Gateway Security Management

400. 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 gateway, and indeed a secure gateway.

401. 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.

## Security Management

402. The previous chapters dealt with the planning and policy framework for establishing a secure gateway. However, it is clear that the security management framework is key to the success of maintaining a secure environment. 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:

i. *Security Administration Tasks*. This includes tasks such as account creation and maintenance, directory list management, access control additions and deletions, key management tasks, certificate or token administration, and system backup. In brief all the "day to day" security tasks that are typical of any IT installation. A feature of these tasks is that some of these tasks are ad-hoc, and others can and are conducted at regular intervals.

ii. *Proactive Security Configuration Checks*. This includes checking critical or important configurations on the gateway. The extent and regularity of the checks will largely be determined by the results of the risk assessment. Obviously, the more critical or high risk an item, the more regular and thorough the checks. The key security configuration parameters should have been determined and documented by the designers as described in Chapter 3. These parameters should be the ones that are regularly checked, in a proactive fashion.

iii. *Proactive Security Audit Checks*. This includes checking user activity on the system, both for users classified as "gateway administrators", and those users that are simply using the gateway. As per the configuration checks, the extent and regularity of the checks will largely be determined by the results of the risk assessment. The tools and methods to be used in conducting this activity should have been determined by the gateway designers.

iv. *Contingency Plans and Tasks*. The will describe the contingency plans and procedures to be followed in event of an actual contingency. It should also outline how the contingency plan is to checked and monitored.

403. The effort that will be spent on each of the components listed above will clearly depend 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.

404. As a guide, it is strongly recommended that the plans and procedures drafted on the basis of the requirements of this chapter be brief and concise. They may be stored on-line in a secure environment, but operators and administrators should 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

405. As stated previously, the security administrative tasks include all the "day to day" tasks that are typical of any IT installation. They need to cover which appointment, under what specific authority, following what specific processes, in what timeframe will complete the stated tasks. **For DSD certification, the following plans and/or procedures marked mandatory or conditional are required to be produced for certification. Also, a clear linkage between gateway policies and the plans/procedures must be clearly evident, as well as demonstrating evidence of implementation.** The following plans and procedures may be covered under the security administration tasks:

i. *Accounts Administration Procedure (mandatory)*. The profile of system accounts, the appointments or staff allowed an account on the system, and how often are old accounts are to be deleted. 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. The procedure should also outline requirements for accounts administration record keeping.

ii. *Privileged Users Plan (mandatory)*. This plan should briefly detail those privileged accounts that are required, and who (by appointment or staff name) is allowed to hold these privileged profiles. The "Account Administration Procedure" should detail how this is to be effected. Privileged accounts management should be derived from the outcomes of the policy (see Chapter 2 - Security Policy). This plan should include password management procedures.

iii. *Access Control Plan and Procedure (mandatory)*. This item 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. This "matrix" will therefore couple those users against those resources that have been agreed and approved by management. The plan should detail the "matrix", and detail the procedure on how to effect 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.

iv. *Key Management Plan and Procedure (conditional)*. Cryptographic key management is crucial to any security environment where they are employed. This plan and procedure document should include how the keys are derived, how often they are changed for each crypto system, the staff that are allowed access and actions to be taken in event of compromise or replacement. This document is mandatory only if cryptographic services are employed as part of the gateway.

v. *Physical Access Plan and Procedure (conditional)*. The plan should detail who is allowed into which door, ie; an access "matrix" similar to the one described above in subparagraph (iii). The procedure should detail how this is to be undertaken. This document is mandatory only if there is an electronic or semiautomatic physical entry access control system. This may include the physical security detection measures, such as an alarm system.

vi. *Backup, Maintenance and Media Control Plan and Procedure (mandatory)*. This should be 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. The frequency of backup, storage or

tapes/disks and period of storage, media reuse/disposal should also be included. The backup plan should include backup or archival of logs or audit trails. The maintenance and media control issues are related in that they both specifically relate to preventing loss of control of key system media.

vii. *User Awareness Plan (mandatory)*. 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 service eg. Logon banners, user access forms, policy documents and user guides, anti-virus software, training.

viii. *Change Management Plan and Procedure (mandatory).* This plan should detail the process by which a change is initiated and approved. Categories of changes need to be identified and those that require a reassessment of the risk assessment should be noted. Notification mechanisms for stakeholders should be outlined.

## Proactive Security Checking Tasks

406. 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 need to 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 required to be checked and the regularity of checking be derived from the "Critical Configuration List" (Chapter 3 – Critical Security Configuration) and the relevant security policy (Chapter 2 - Security Policy).

407. **For DSD certification, only those plans or procedures marked mandatory are required. Also, a clear linkage between gateway policies and the plans/procedures must be clearly evident, as well as demonstrated evidence of implementation.** Reports should be by exception, so as not to overload the recipient of the report with an inordinate amount of material to analyse. DSD 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 are required to cover the following areas:

iv. *Firewall Configuration Checking Plan and Procedure (mandatory)*. 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 this is to be undertaken.

v. *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.

vi. *Crypto Configuration Checking Plan and Procedure (conditional).* This document would include cryptographic issues 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 cryptographic systems are employed as part of the gateway.

vii. *Alarm and Access Control Plan and Procedures (optional).* 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

408. 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 need to 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 (Chapter 3) and the relevant security policy (Chapter 2 - Security Policy).

409. Reports should be by exception, so as not to overload the recipient of the

report with an inordinate amount of material to analyse. DSD will pay particular attention to the reports, to ensure they are readable and do not place an undue burden on the recipient. **For DSD certification, only those plans or procedures marked mandatory are required. Also, a clear linkage between gateway policies and the plans/procedures must be clearly evident, as well as evidence of implementation.**

i. *Real Time Reporting Plan and Procedure (mandatory).* This document should be based on the objectives of the "Incident Detection and Response Policy", and the gateway design documentation. The objective here 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 security integrity of the gateway.

ii. *Off-Line or Analytical Reporting Plan and Procedure (mandatory).* This document should be based on the objectives of the "Incident Detection and Response Policy", and the gateway design documentation. The objective here 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. As previously mentioned, DSD and connected customers are to be an information addressee on these reports, for DSD certified systems.

## Contingency Plan

410. DSD will not be requiring any minimum standards, or preset plans or procedures. However, it is strongly recommended that all plans and procedures produced are directly related to the outcomes of the gateway policy and design tasks, and therefore derived from the results of the risk assessment.

## Incident Response Plan and Procedures

411. These could be covered in the Contingency Plan or separately. The Incident Response Plan and Procedures will describe the steps to be followed when the proactive security checking tasks and audit tasks identify a security incident. 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 need to be outlined in relation to each category of incident. The appointment(s) responsible for performing incident response also need to be clearly identified. It is strongly recommended that all plans and procedures produced are directly related to the outcomes of the gateway policies and therefore derived from the results of the risk assessment.

# Chapter 5
# DSD Certification Procedures

501. As discussed at the beginning of this manual, DSD gateway certification is provided as an independent service to verify that a gateway is being managed as per the requirements of this document. It should be stressed at this stage that this certification process does not provide any guarantee that the gateway manager will always comply with the requirements of this document. However, DSD checks will provide a degree of assurance that management processes are satisfactory for the continued, secure operation of the gateway.

## Certification Process

502. The certification process can be broken down into five distinct phases as follows:

ii. *Review of Risk Assessment*. It is recommended that the risk assessment be in accordance with the requirements of Chapter 1, but it need not be. The primary outcome of the risk assessment phase is to provide a list of prioritised countermeasures.

iii. *Review of Policy Documentation*. Based on the outcomes of the risk assessment, Access, Security, Contingency and Incident Detection and Response Policies should be formulated.

iv. *Review of Design Documentation*. The design phase may produce a number of documents some of which will not be directly related to security functionality. Those required for certification include the Gateway Logical/Infrastructure Diagram, Concept of Operations, List of Mandatory Requirements, Risk Based Requirements and List of Critical Configurations.

v. *Review of Plans and Procedures*. These include Security Administrative Tasks, Proactive Security Checking Tasks, Proactive Security Auditing Tasks and the Contingency Plan.

vi. *Review of Current Configuration*. This includes configuration checking of critical components, verifying that the tools in use meet the requirements and are usable. The items listed in Annex A are an indication of those items that may be checked. As an indication a small site may be checked in 2 – 3 days.

503. As part of the review of the above documents, DSD will specifically look for inconsistencies, indications that minimum standards have 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. Annex B contains a detailed listing of

the components required for each phase of the certification process. These steps are discussed in detail in the previous chapters.

## Conditions of Certification

504. DSD will provide, on a fee for service basis, certification for the following gateway environments:

i. Government agencies developing gateways that will connect from HIGHLY PROTECTED or lower; or RESTRICTED or lower; networks, to public networks such as the Internet. DSD will not certify gateways where networks processing material rated at higher classifications or categories are connected to public networks.

ii. Companies wishing to provide gateway services to Government clients will be provided an entry-level certification until a Government client has been signed up. The requirements for entry level certification are detailed further in this chapter.

iii. Service providers who, via outsourcing contracts, are required to provide gateway services to their clients. In these cases, the Agency contract controller becomes the DSD customer, and any problems with the certification or issue of the certification will be passed to the contract controller. This type of certification does NOT enable an outsourcing partner to claim DSD certification when offering services to other agencies/clients, unless specific agreement has been obtained from the contract controller.

iv. Government agencies developing gateways not connecting to public networks, where the level of risk warrants a certified gateway. This requirement should be discussed with DSD, in the first instance.

## Types of Certification

505. 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:

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

ii. Regular advice to DSD on the analysed threat level.

506. **Provisional Certification** is awarded to those environments that are lacking compliance in some aspect(s) of the design, policy or management. This certification does not preclude the gateway from operating, but does mandate that these problems be corrected within an appropriate timeframe. This timeframe will be advised in the letter of certification, for those sites where this is an issue. Failure to correct the anomalies in the stated timeframes will result in DSD withdrawing the certification.

507. **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 provisional on an additional certification check within a short timeframe of a Government client being connected. This will be advised via the certification letter. All aspects detailed in Annex A are expected to be met as part of the entry–level certification. Those companies that do not have infrastructure in place should not seek an entry-level certification until this is so.

508. **Recertification** is undertaken on all certified sites at least every 12 months or at initiation of a major change. A major change can include:

- Change of ownership
- Significant redesign of gateway architecture
- Significant change in access policy
- Upgrade of hardware and software
- Installation of additional services
- Addition of clients

Depending on the nature of the change, a change may be able to occur without recertification, but may require DSD review. DSD will review change management procedures as part of the certification process. DSD will provide assistance to organisations to identify significant changes and to develop procedures to notify the reviewer (DSD) as part of the change management process.

# Annex A

# Example Risk Assessment

NOTES:

1. This is provided as an **EXAMPLE ONLY**, for guidance purposes. Gateway designers are not to "cut and paste" information from this table.
2. The entries in this table have been graded on the level of the Countermeasure Priority Rating (column 7).

| *Column 1*<br>***Asset Identification*** | *Column 2*<br>***Threat to the Asset*** | *Column 3*<br>***Threat Likelihood*** | *Column 4*<br>***Harm, if threat is realised*** | *Column 5*<br>***Resultant Risk*** | *Column 6*<br>***Required Risk*** | *Column 7*<br>***Countermeasure(s) Priority Rating*** |
|---|---|---|---|---|---|---|
| ***Row 1.*** **Protection of sensitive emails on the internal network** | Inadvertant distribution of sensitive email to outside addressee | *Very High* | *Serious* | *Extreme* | *Nil* | **5** |
| ***Row 2.*** **Availability of hardware infrastructure** | Accidental electrical power failure | *Medium* | *Grave* | *Critical* | *Nil* | **4** |
| ***Row 3.*** **Availability of email services, by gateway customers** | IP based "Denial of service" attack on the mail host | *Extreme* | *Damaging* | *Critical* | *Low* | **3** |
| | "Mail Bomb" attack on the mail host | *Very High* | *Damaging* | *Critical* | *Low* | **3** |

Table continued over page

| *Column 1*<br>***Asset Identification*** | *Column 2*<br>***Threat to the Asset*** | *Column 3*<br>***Threat Likelihood*** | *Column 4*<br>***Harm, if threat is realised*** | *Column 5*<br>***Resultant Risk*** | *Column 6*<br>***Required Risk*** | *Column 7*<br>***Countermeasure(s) Priority Rating*** |
|---|---|---|---|---|---|---|
| ***Row 4.*** **Integrity of firewall access rules, and thus security of internal network services and resources** | Accidental misconfiguration of firewall rules | *Low* | *Serious* | *High* | *Nil* | **3** |
| ***Row 5.*** **Secure access control to the physical building, and thus the infrastructure** | Loss or theft of access control token allows unauthorised access | *Low* | *Serious* | *High* | *Nil* | **3** |
| ***Row 6.*** **Secure access control to the electrical distribution panel/system, or any component of it (excluding UPS)** | Inadvertant power outage due to accidental tampering with distribution system(s) | *Low* | *Grave* | *High* | *Low* | **2** |
| ***Row 7.*** **Integrity of publicly available web information** | Loss of confidence or goodwill due to "hacking" of web page | *High* | *Minor* | *Medium* | *Low* | **1** |
| ***Row 8.*** **Secure access to internal networks by authorised staff, from the external network(s)** | Loss of crypto token or keys required to access the secure channel(s) | *Very Low* | *Serious* | *Medium* | *Low* | **1** |

# Annex B

# List of DSD Certification Requirements

## 1. Review Risk Assessment Documentation

*Policy documentation should be no more than 5-10 total pages in length, as a guide.*

The risk assessment should provide enough detail to guide the priority of the countermeasures. It need not be in accordance with Chapter 1, but that is recommended.

## 2. Review Policy Documentation

Policy documentation should be no more than 10 –15 total pages in length, as a guide. *Minimum policy standards are contained throughout the discussions in Chapter 2, and are summarised at the end of Chapter 2.*

i. Review the "Access Policy", including any referenced client documents

ii. Review the "Security Policy"

iii. Review the "Contingency Policy"

iv. Review the "Incident Detection and Response Policy"

## 3. Review Design Documentation

*Design documentation should be no more than 10 –15 total pages in length, as a guide.*

i. Review the "Gateway Logical/Infrastructure Diagram"

ii. Review the "Concept of Operations"

iii. Review "List of Mandatory Requirements"

iv. Review "Risk Based Requirements"

v. Review "List of Critical Configurations"

## 4. Review Plans and Procedures Documentation

i. Review the "Security Administration Tasks"

ii. Review the "Proactive Security Checking Tasks"

iii. Review "Proactive Security Audit Tasks"

iv. Review "Contingency Plan"

## 5. Configuration Checking

*The following is produced, as a guide. It is expected that the configuration checking for a small site may take 2 –3 days.*

i. Review Firewall Configurations

ii. Review Proxy Configurations

iii. Review Security checking tools and configurations

iv. Review Security audit tools and configurations

v. Review Physical Security