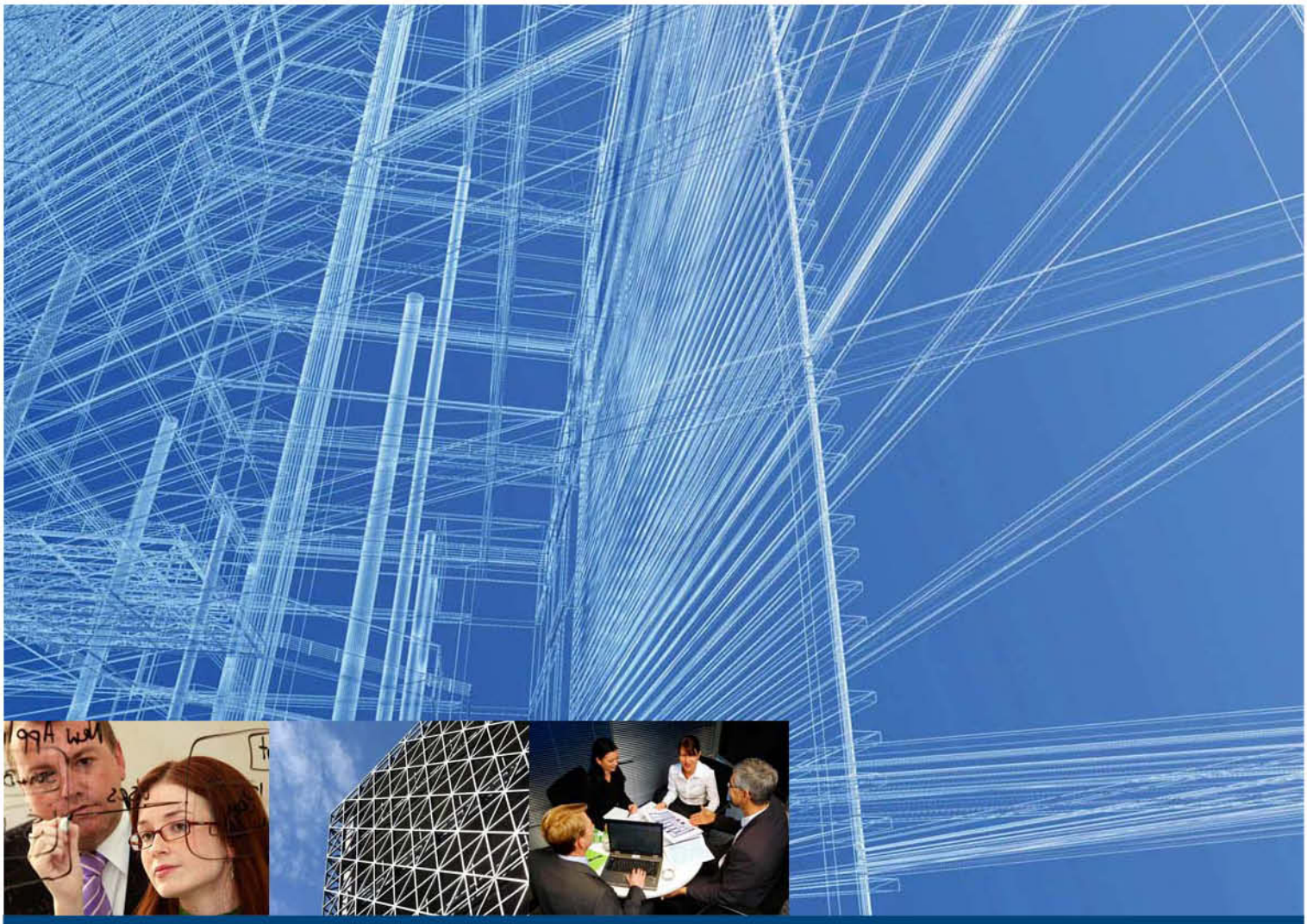

Deployment of intrusion detection and prevention systems guideline

Final

September 2011

v1.0.0

PUBLIC

Queensland Government Enterprise Architecture

Queensland Government Chief Technology Office
Department of Public Works

Queensland Government

Document details

Security classification	PUBLIC		
Date of review of security classification	September 2011		
Authority	Queensland Government Chief Information Officer		
Author	Queensland Government Chief Technology Office		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Executive Director
Queensland Government Chief Technology Office
qgcto@qld.gov.au

Acknowledgements

This version of the *Deployment of intrusion detection and prevention systems guideline* was developed and updated by Queensland Government Chief Technology Office.

Feedback was also received from a number of staff from various agencies, which was greatly appreciated.

Copyright

Licence

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

Figures

Tables

1 Introduction

1.1 Purpose

The Deployment of intrusion detection and prevention systems (IDPS) guideline, is structured to assist agencies with the development, implementation and management of IDPS, within the agency's Information and Communication Technology (ICT) environment. This guideline is intended to maintain consistency and support where possible, with the Information Standard 18: Information Security (IS18).

A QGEA guideline is non-mandatory and provides information for Queensland Government agencies on the recommended practices for a given topic area.

1.2 Audience

This document is primarily intended for:

- agency staff and operational areas involved in intrusion detection and prevention services
- agency information security management
- information security governance bodies.

1.3 Scope

This guideline relates to the best practice for deployment of IDPS and is product/vendor independent.

2 Background

2.1 Why was this guideline developed?

The Auditor General of Queensland's Report to Parliament No. 4 for 2009 detailed a number of key network security issues (outlined in Section 4.2 – Information Technology Network Security). With regards to intrusion detection and prevention systems, the report found that agencies do not have intrusion detection and prevention systems implemented or had limited automated intrusion monitoring capabilities.

This guideline has been developed to assist agencies to establish and implement a strategy for the deployment and management of intrusion detection and prevention systems. For those agencies that already have intrusion detection and prevention systems in place, this guideline will assist when conducting reviews or increasing ICT monitoring to ensure the approach is comprehensive.

2.2 Relationship to other QGEA documents

This guideline complies with the implementation of Information Standard 18. In particular, it adheres to the principles relating to:

- incident management
- communications and operations security management
- compliance management.

This guideline will assist agencies to meet their requirements for event and incident management, internal and external, as defined by the Queensland Government Information Security Event and Incident Management Guideline.

In addition, this guideline complements the Queensland Government Information Security Classification Framework and Queensland Government Network Transmission Security Assurance Framework by defining specific controls that will assist in implementing an additional layer of protection, for the agency's information, information systems and ICT assets.

3 IDPS purpose

The purpose of the IDPS is to monitor the network traffic beyond traditional firewall capabilities to ensure network attacks such as man in the middle, viruses, and malware are detected and a set of pre-defined actions are initiated. In some instances, a single IDPS technology may not adequately address and satisfy the requirements as such a combination of the technology may be required.

In the broader context of information security management, IDPS is only one part of the agency's information security strategy, and should be built around the principle of defence in depth to support other implemented security controls. Therefore, to detect and prevent a threat from occurring, multiple layers (or controls) should be implemented.

IDPS can be utilised for the following functions:

- identifying and preventing possible attacks/threats
- reporting of the attacks/threats
- identifying security policy problems
- recording information related to observed events.

4 IDPS types

There are two main types of IDPS, the intrusion detection system and the intrusion prevention system.

Intrusion detection systems automate the monitoring process to analyse traffic for suspicious behaviour that is occurring within the monitored location, either on a host or specific network segment. Intrusion detection systems are not designed to prevent a suspicious behaviour or threat, but are used as a passive system to only detect and alert on the activity.

Intrusion prevention systems provide similar functionality to intrusion detection systems, however the key difference is that prevention systems are designed to be a reactive system, to prevent the detected threat or activity from happening when implemented inline in a network path or on a specific host. Therefore, if a specific attack is occurring, it will be detected, alerted and a pre-defined action will occur, such as, denying the attack.

In addition, IDPS can be either a device or a software application.

Important note: Intrusion detection and prevention systems cannot inspect encrypted traffic, therefore the traffic can only be inspected via a host- or network-based system when the traffic is decrypted.

These systems can be separated into the following categories:

4.1 Host-based

Host-based analyses malicious activity within a particular system (installed on individual workstations and/or servers) including system logs, running processes, connected portable media, file access and modification, and system and application configuration changes. Host-based IDPS are most commonly deployed on critical hosts such as internet facing servers and servers containing sensitive information.

Typically, host-based prevention systems deny attacks by utilising various methods such as, preventing the creation or changes to files or applications/code from executing.

4.2 Network-based

Network-based analyses traffic over a specific network segment for malicious activity. It is most commonly deployed at a boundary or internal networks, such as in the gateway perimeter or internal network server segments.

Typically, network-based prevention systems deny attacks by dropping traffic or sending Transmission Control Protocol (TCP) resets. When dropping traffic, the connection will not continue, however, the hosts communicating will attempt to continue exchanging data until the connection will eventually timeout. TCP resets will reset the connection between the communicating hosts.

4.3 Specialised classes

Within the previously mentioned two main types of IDPS, there are a number of specialised sub classes that have evolved to provide monitoring additional capabilities in specific architectures. These specialised sub classes include wireless, network behaviour analysis (NBA) and hypervisor-based.

4.3.1 Wireless

Wireless IDPS monitors and analyses wireless radio spectrum traffic for malicious activity and unauthorised wireless access points. It is most commonly deployed within range of the organisation's wireless network to monitor, but can also be deployed to locations where unauthorised wireless networking could be occurring.

4.3.2 NBA

NBA analyses network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, malware (such as worms, backdoors), and policy violations (such as a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on to internal networks, and can be deployed where they can monitor flows between internal and external networks (such as the Internet and business partners networks). However, NBA systems are typically a technique used within and in conjunction of IDPS.

4.3.3 Hypervisor-based

Hypervisor-based IDPS monitors and detects threats targeted within the virtualised environment at the hypervisor layer. The hypervisor is responsible for managing guest operating system access to hardware, for example CPU, memory, storage and network interface cards (NICs). Traditional host-based intrusion systems can be installed on each virtual machine, however, this will not provide the appropriate protection of the virtual fabric composed of the hypervisor, management stack and virtual switch.

5 Detection methods

Intrusion systems have different methods for detecting suspicious behaviour. Each method has its advantages and disadvantages, and should be aligned with the security requirements of the proposed implementation. Typically, IDPS use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. Listed below are the common and widely available detection methods.

5.1 Signature-based

- Signature-based detection methods compare monitored traffic to known threat signatures. This process is similar to the functionality of traditional antivirus software.
- Considerations:
  - signatures must be continuously updated from the specific vendor provider
  - cannot identify new attacks such as zero day exploits, therefore relies on continuous updates
  - identified attacks must have a known signature.

5.2 Anomaly-based

- Behavioural-based system that learns the 'normal' activities of an environment, to identify unknown activity. The detection method is based on heuristics or rules, rather than patterns or signatures.
- Considerations:
  - can detect new attacks
  - anomaly-based can also be called behaviour- or heuristic-based
  - anomaly-based detection relies on the intrusion system learning the environment, to build a profile
  - requires much more overhead and processing capacity than signature-based
  - can generate a large number of false positives.

5.3 Stateful packet inspection

- Stateful protocol analysis examines different parts of the protocol for anomalous behavior or exploits against predetermined profiles of generally accepted definitions of protocol activity for each protocol state.
- Considerations:
  - it is capable of understanding and tracking the state of protocols that have a notion of state, which allows it to detect many attacks that other methods cannot
  - unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used

  - difficult to develop completely accurate models of protocols
  - resource-intensive and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

6 IDPS components

The typical components that consist of an IDPS solution are:

- Sensor or Agent:
  - Sensors and agents monitor and analyse activity. The term sensor is used for IDPS that monitor networks, including network-based, wireless, and network behaviour analysis technologies. The term agent is typically used for host-based IDPS technologies.
- Management Server:
  - A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis and correlation of collected event information that the sensors or agents provide.
- Database Server:
  - A database server is a repository for event information recorded by sensors, agents, and/or management servers.
- Console:
  - A console is an application or device that provides an interface to manage the IDPS.

7 Comparison of IDPS systems

IDPS types	Types of malicious activity detected	Scope	Strengths
Network-based	Network, transport, and application TCP/IP layer activity.	Multiple network subnets, segments and groups of hosts.	Able to analyse the widest range of application protocols; only IDPS that can thoroughly analyse many of them.
Host-based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity.	Individual hosts.	Only IDPS that can analyse activity that was transferred in end-to-end encrypted communications and monitor activity within a particular system such as system logs, running processes, connected portable media, file access and modification, and system and application configuration changes.

IDPS types	Types of malicious activity detected	Scope	Strengths
Wireless	Wireless radio spectrum; presence of unauthorised access points.	Multiple WLANs and groups of wireless clients.	Only IDPS that can monitor wireless radio spectrum activity.
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows.	Multiple network subnets, segments and groups of hosts.	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections.
Hypervisor-based	Host application, operating system (OS) and virtualised activity.	Multiple virtualised environments.	Monitor and detect threats at hypervisor layer within a virtualised environment.

Table 1 – Comparison of IDPS systems

8 IDPS Strategy

For IDPS to have maximum effectiveness in assisting to protect agencies' information assets and information systems, a number of key steps need to be taken to ensure the solution meets the agency's requirements, and the capabilities of the system are fully utilised. The following is a guideline of the steps required.

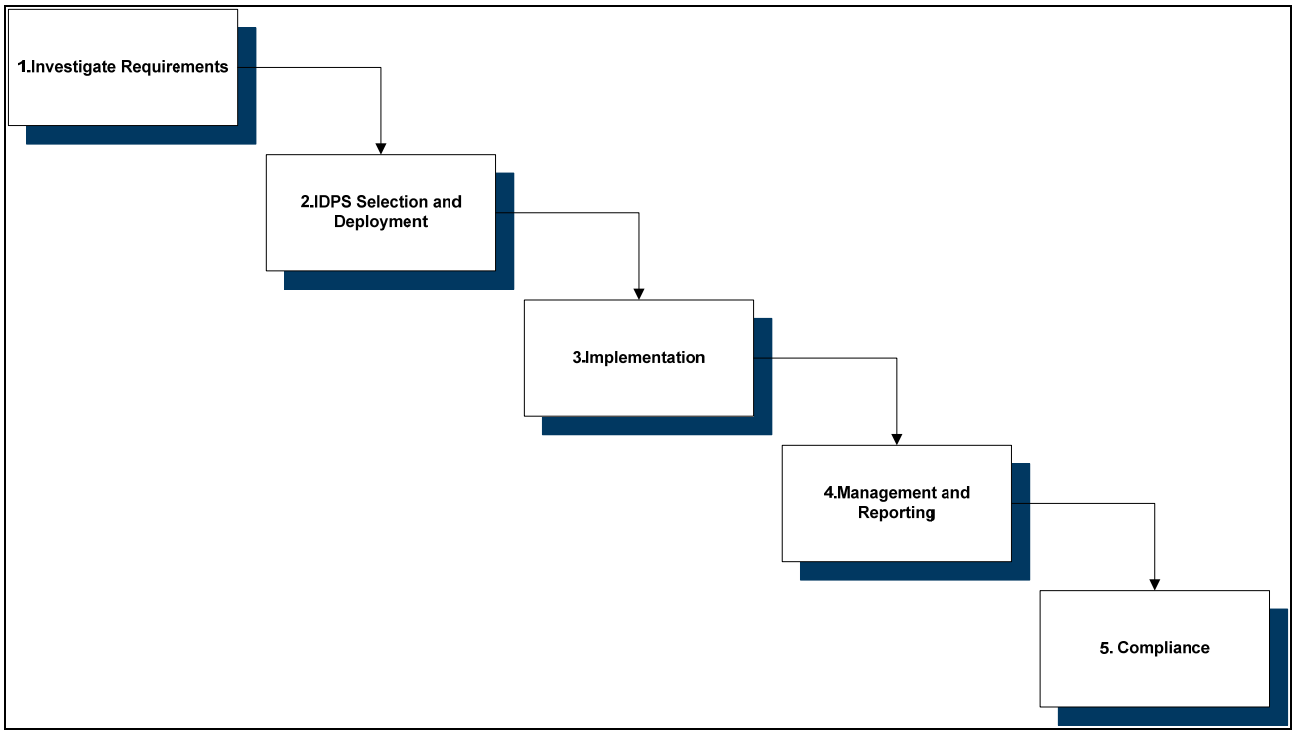

Figure 1 – Intrusion system strategy steps

8.1 Investigate requirements

During the investigation phase the agency must have and/or fully understand the following:

- agency's risk management methodology
- agency's security objectives
- agency's information security policies, Queensland Government legislative and information standards requirements.

To assist management in the decision making process, a threat and risk assessment must be completed as per the agency's risk management framework. This will formally identify the agency's risks and produce a recommended mitigation strategy to ensure the agency risk profile is maintained. If the agreed mitigation strategy includes a need for an IDPS solution, the agency should progress to the next step of IDPS Selection and Deployment.

8.2 IDPS selection and deployment

The second step is to identify the specific type of IDPS, deployment and detection method. This will need to be aligned with the agency's business and security requirements. Therefore, the agency must be fully aware of possible impacts to the operations of the business, performance and network architecture model. IDPS are capable of performing a number of detection methods. Therefore, it is important to identify the most feasible type of IDPS for the desired security requirements.

When designing for the implementation of an IDPS, it should be included as part of the agency network and server architecture model. This is to ensure that the IDPS monitors the appropriate network traffic effectively and efficiently. In addition, any potential issues should be identified for integrating different systems and/or providers.

The recommended locations for IDPS are:

- sensitive or security classified infrastructure (such as hosts, networks and information assets/systems)
- agency gateway perimeters and semi-trusted networks.

It is not recommended to implement an IDPS in un-trusted (external) networks, such as the Internet, due to the level of noise that will be generated, unless is it positioned behind an access control device (i.e. firewall or screening router).

While the agency must endeavour to apply its network security policies to all segments of the agency network, it must define the required depth of defence on internal networks, in line with their business, corporate and IT policies.

Agencies should consider the following considerations for sensors:

- costs associated with the deployment, maintenance, and monitoring of sensors
- operating systems and applications supported by the sensors
- ability of the infrastructure to support the sensors for required network bandwidth utilisation
- define a monitoring period to assess potential impacts as part of the design and tuning configuration
- investigate standardisation of work practices to reduce the amount of exceptions needed for 'business as usual' requirements.

8.2.1 Host-based

As mentioned previously host-based IDPS agents are most commonly deployed to critical hosts such as internet facing servers, servers containing sensitive information and end user devices. Host-based provide additional layer of protection that can be used in combination to complement other intrusion systems or controls, depending on the agency's business and security requirements. It is important to remember that host-based solutions will only inspect traffic from or to the monitored host, including system activities.

8.2.2 Network-based

Network-based sensors are utilised for the monitoring of specific segments or larger portions of a network, as opposed to deploying host sensors (depending on requirements).

Network sensors can be deployed in the following modes:

- Inline: In inline sensor is deployed so all network traffic it is monitoring passes through the sensor, typically these sensors can be integrated in firewalls appliances. The purpose of deploying inline sensors is to deny detected attacks from occurring or perform another pre-defined action. IPS sensors are typically implemented in the gateway perimeter environment or between internal networks. The following is a list of considerations for deploying inline, which need to be further investigated as per the agency's security and business requirements:
  - When configured to be inline of the traffic flow and the intrusion system was to fail, the sensor can be configured to fail-open (allowing traffic to pass) or fail-close (denying traffic). In addition, when a sensor is configured inline, it will need to be able to handle the performance throughput requirements, as all traffic (depending on policy) is been inspected in real-time.
  - The sensor may falsely detect permitted traffic (false positive) and incorrectly deny the traffic.
  - Initial deployment could be configured in a two phase approach. For example, step 1, configure in IDS mode, to learn the environment, then step 2, change over to IPS mode.
  - Deploying a sensor which is directly internet-facing may generate a large number of events and unnecessary processing utilisation which is not appropriate. Therefore, it would be recommended to implement behind an access control device such as a firewall or be integrated into the firewall and configured to only inspect allowed traffic (depending on the business and security requirements).
- Passive: A passive sensor is deployed so that it monitors a copy of the actual network traffic; no traffic actually passes through the sensor. Therefore, it is possible to perform more detailed analysis, since it is not been done in real time. Passive sensors are typically deployed so that they can monitor specific network segments, which is more cost effective. Passive sensors can monitor traffic by integrating with existing infrastructure, via span ports or network taps.
  - Span Port: Span ports are usually available on existing network infrastructure for the ability to monitor all network traffic going through the device. Therefore allowing a sensor to be connected and monitor traffic. Span ports can be resource-intensive; which means when under heavy load, the span port might not be able to see all traffic, or be temporarily disabled. Also, devices may have a limited number of span ports which may be required for the use of other monitoring devices such as network performance monitoring.

– Network Tap: A network tap is a direct connection between a sensor and the physical network media itself. The tap provides the sensor with a copy of all network traffic being carried by the media. Installing a tap generally involves some network downtime, and problems with a tap could cause additional downtime. Also, unlike span ports, which are usually already present throughout the infrastructure, network taps need to be purchased as add-ons to the network.

8.2.3 Deployment example – gateway perimeter

The following diagram identifies the recommended locations for the gateway perimeter environment:

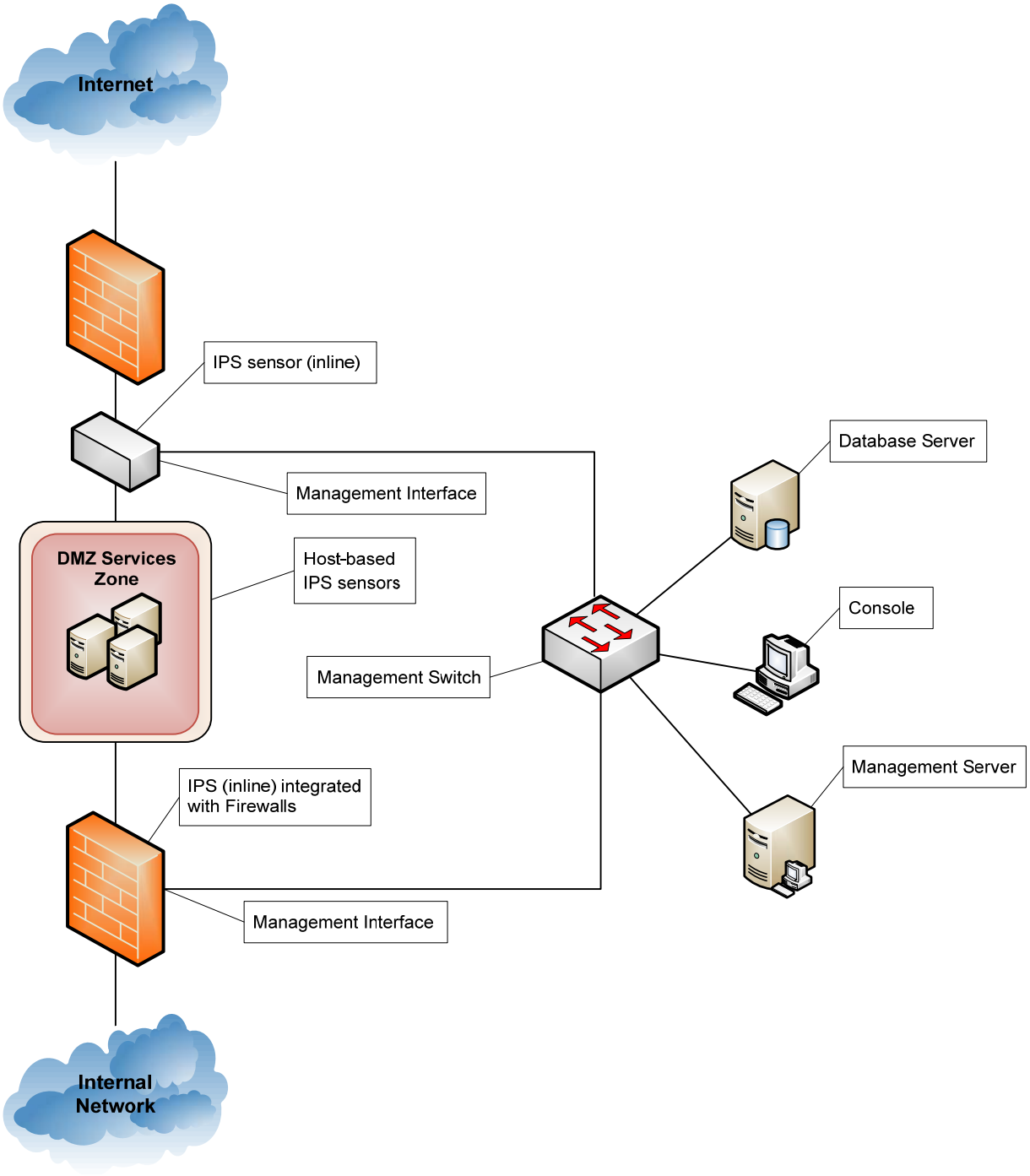

Figure 2 – Deployment example – gateway perimeter

8.2.4 Deployment example – internal network

The following diagram identifies the recommended locations for the internal network environment:

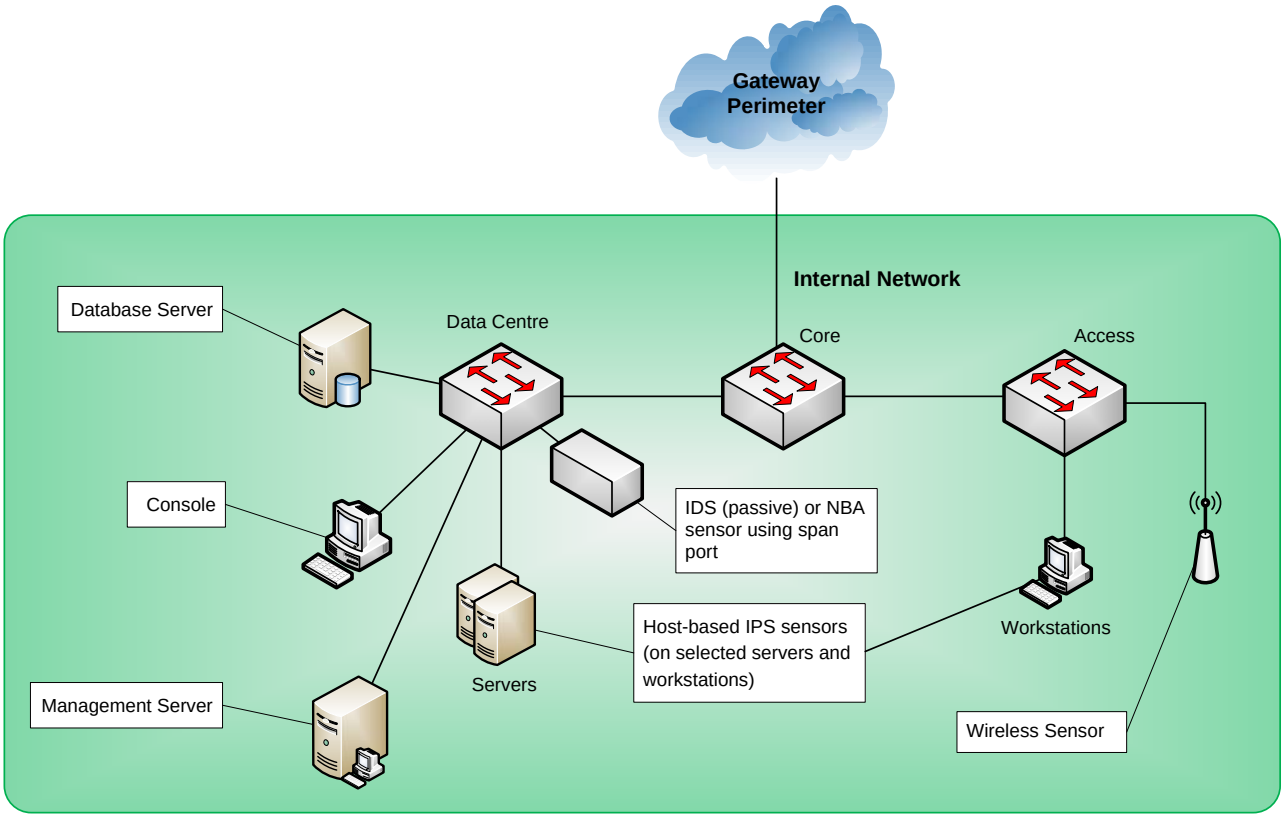

Figure 3 – Deployment example – internal network

8.3 Implementation

Although there are a number of administrative and technical requirements for the implementation of an intrusion system, this section only highlights the most important aspects. All IDPS solutions design and configuration should be managed by the agencies risk management framework.

- Roles and responsibilities:
  - Agency roles and responsibilities policy must include the roles for the management and incident response for the intrusion system.
  - Operational staff must be aware of the agency's incident management policy and procedures, so detected incidents are responded to, reported and escalated correctly. This should be guided by the Queensland Government Information Security Event and Incident Management Guideline.
- Detection Method Settings:
  - All IDPS policies are required to be carefully managed and configured (or tuned) for the specific function of the solution. This is necessary to minimise any negative impact or false alerting. It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other. Many organisations choose to decrease false negatives

at the cost of increasing false positives, which means that more malicious events are detected but more analysis resources are needed to differentiate false positives from true malicious events. However, this decision should be based on the agency's risk management framework and security classification.
  - Examples of the tuning process are, enabling or disabling signatures, modifying signature settings and changing sensitivity levels of behaviour- or heuristic-based systems on a per policy and monitored interface basis.
- Alerting configuration:
  - Automate monitoring for intrusions and security breaches.
  - Implement alarms for detected breaches and intrusion attempts, and define response processes.
  - Consider integrating with other agency alerting systems.
- Reporting:
  - Ideally, the IDPS should be integrated into the agency's security information and event monitoring solution, to provide centralised automated monitoring and event correlation reporting capabilities. This centralised repository should include logs from the agency's firewalls and other security devices.

8.4 Management and reporting

Intrusion systems must be managed effectively to ensure that detected events and incidents are immediately responded to and reported as per Queensland Government, and where relevant, Federal requirements. In addition, the security incident must be contained and managed to reduce the impact of the incident across the agency's information systems. The following is a list of items to assist in meeting this requirement:

- agency staff must be aware of their responsibilities and procedures for the timely detection, escalation and reporting of security events and incidents
- within the agency's organisation structure, there should be separation of duties for the management of and reporting from IDPS, this is to reduce the opportunity for process subversion
- incident management policies and procedures must be established to review violations to ensure appropriate responses in the event of security incidents
- detected events and incidents should be managed through the agency's information security policies and incident management procedures that are supported through technology-based controls such as security information and event management (SIEM) solutions
- comply with Queensland Government reporting requirements, such as:
  - Queensland Government Information Security Event and Incident Management Guideline
  - Queensland Government Information Security Incident Category Guideline
  - Queensland Government Information Security Event and Incident Reporting Standard.

8.5 Compliance

To ensure that the implemented IDPS is working as per design and requirements, it is necessary to perform periodic reviews and compliance audits of the intrusion system by personnel not responsible for day to day support and management of IDPS. This should be performed annually via the following processes:

- threat and risk assessments reviews
- configuration/audit reviews
- penetration testing.

This will assist the agency to confirm the control effectiveness for the specified risks for protecting the agency's information systems. These annual reviews should be completed in line with Queensland Government compliance requirements. In addition, agencies must be able to demonstrate that reviews are occurring.