Hardware Recommendations for establishing a National CIRT in <COUNTRY>

TABLE OF CONTENTS

1 INTRODUCTION

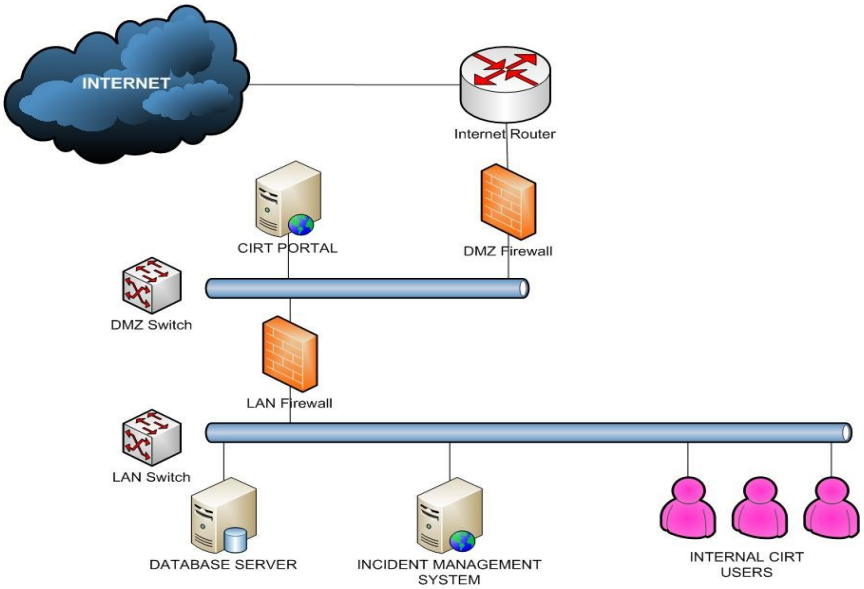
The following sections in this document detail out the Network and Server Hardware recommendations. They are categorized in three designs as detailed below;

a. Basic Design – comprises of the bare minimum requirements for setting up and operating a National CIRT
b. Expansion Design – comprises of a recommended requirement for setting up and operating a National CIRT
c. HA (High Availability) Design – comprises of a fail over modal to maintain a high availability and operation of the National CIRT

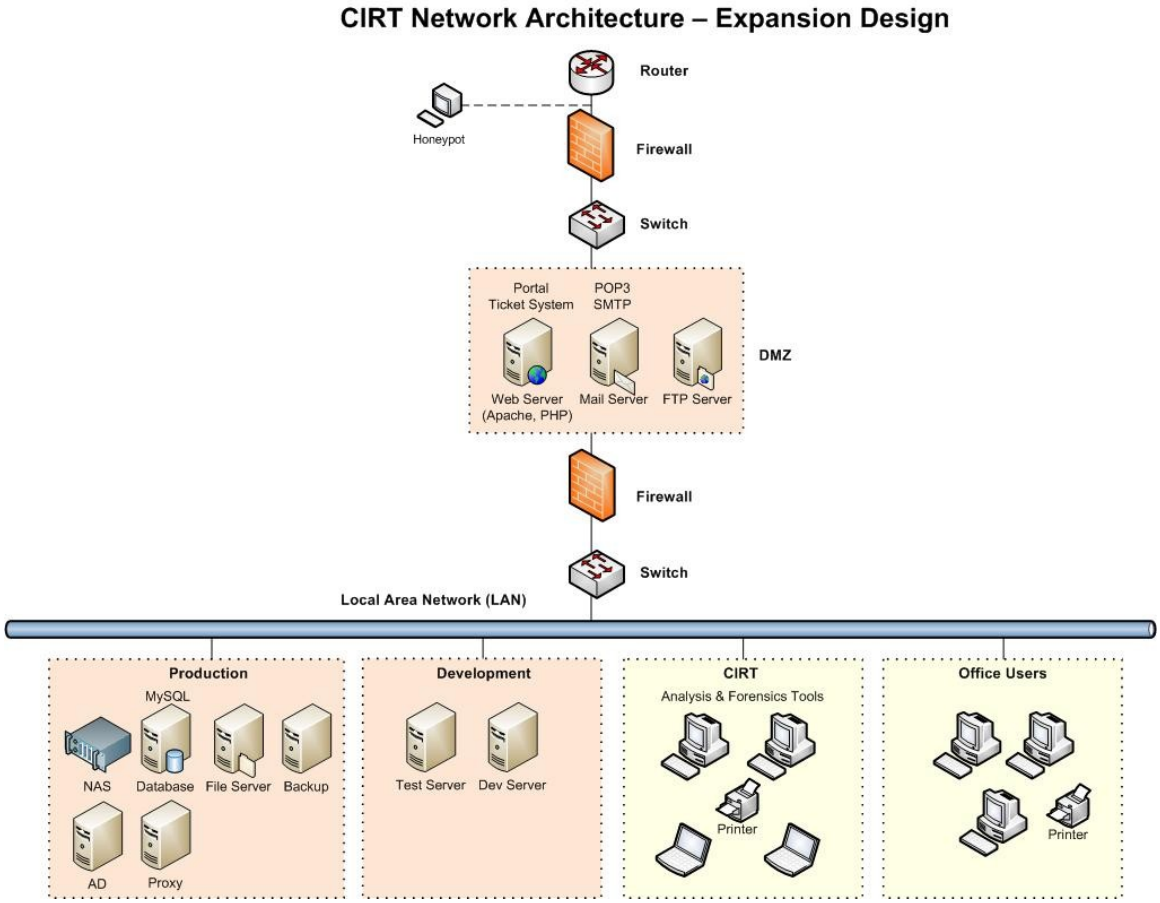
2 TECHNICAL ARCHITECTURE

The three proposed network designs are depicted in this section as below;

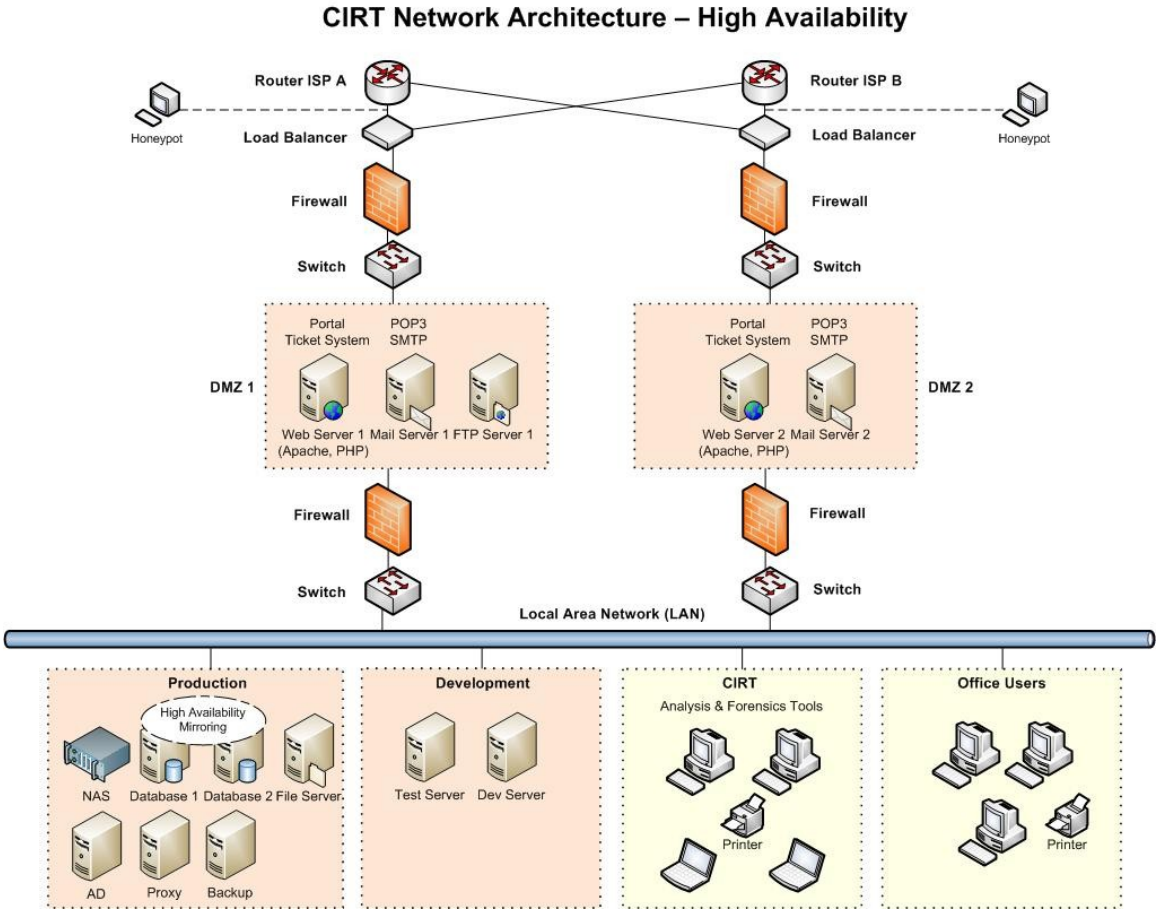
2.1 Basic Design



2.2 Expansion Design



2.3 High Availability Design



3 HARDWARE INVESTMENT

3.1 Basic Design

Hardware	Services	Number of Units
Router	Connection to ISP	1 unit
Firewall	DMZ & LAN Firewall	2 units
Switch	DMZ & LAN Layer 2 Switch	2 units
Server 1	CIRT Portal (Web) Server	1 unit
Server 2	Database Server	1 unit
Server 3	Incident Management System Server	1 unit
Laptop	Incident Management Activities	3 units *
Desktop	Normal Office Activities	3 units *
Printer	Networked Laser Printer	1 unit *

* The numbers may vary depending on team size.

3.2 Expansion Design

Hardware	Services	Number of Units
Router	Connection to ISP	1 unit
Honeypot Server	Honeypot Services	1 unit
Firewall	DMZ & LAN Firewall	2 units
Switch	DMZ & LAN Layer 2 Switch	2 units
Server 1	CIRT Portal (Web) Server - Ticketing System	1 unit
Server 2	Mail Server - POP, SMTP	1 unit
Server 3	FTP Server - File Transfer	1 unit
Server 4	Database Server - MySQL	1 unit
Server 5	File Server	1 unit

Server 6	Backup Server	1 unit
Server 7	Active Directory Server	1 unit
Server 8	Proxy Server	1 unit
Server 9 (Optional)	Development Server	1 unit
Server 10 (Optional)	Testing Server	1 unit
Storage	Network-attached Storage (NAS) - RAID Array Configuration	1 unit
Laptop	- Incident Management Activities - Analysis and Forensics	3 units*
Desktop	Normal Office Activities	3 units*
Printer	Networked Laser Printer	2 units*

* The numbers may vary depending on team size.

3.2.1 Assumptions

Server 7 and Server 8 (Active Directory Server and Proxy Server) are included in this diagram with the assumption that the said servers are not present in the existing office network. If the servers are already present, then these 2 servers can be omitted from the list above.

Server 9 and Server 10 (Development Server and Testing Server) are mainly for the further development and testing of the CIRT application. These are optional components that will give added value to the development of services offered by the upcoming CIRT but are not key to the deployment of a CIRT. Nevertheless, these optional components will contribute in later phases of a CIRT.

It is also assumed that the backup server will consist of an array of Tape Storage that will follow an agreed procedure and allow for full backup and restore. The procedure will also contain processes for storing tape backup in different locations to allow for Disaster Recovery. A Disaster Recovery Proposed Network Diagram is shown in Section 4 below.

3.3 HA Design

Hardware	Services	Number of Units
Router	Connection to ISP	2 units
Honeypot Server	Honeypot Services	2 unit
Load Balancer	Distribute Network Workload	2 units
Firewall	DMZ & LAN Firewall	4 units
Switch	DMZ & LAN Layer 2 Switch	4 units
Server 1	CIRT Portal (Web) Server - Ticketing System	2 unit
Server 2	Mail Server - POP, SMTP	2 unit
Server 3	FTP Server - File Transfer	1 unit
Server 4	Database Server - MySQL - Mirrored	2 unit
Server 5	File Server	1 unit
Server 6	Backup Server	1 unit
Server 7	Active Directory Server	1 unit
Server 8	Proxy Server	1 unit
Server 9 (Optional)	Development Server	1 unit
Server 10 (Optional)	Testing Server	1 unit
Storage	Network-attached Storage (NAS) - RAID Array Configuration	1 unit
Laptop	- Incident Management Activities - Analysis and Forensics	3 units *
Desktop	Normal Office Activities	3 units*
Printer	Networked Laser Printer	2 units*

* The numbers may vary depending on team size.

3.3.1 Assumptions

Server 7 and Server 8 (Active Directory Server and Proxy Server) are included in this diagram with the assumption that the said servers are not present in the existing office network. If the servers are already present, then these 2 servers can be omitted from the list above.

Server 9 and Server 10 (Development Server and Testing Server) are mainly for the further development and testing of the CIRT application. These are optional components that will give value to the upcoming CIRT but are not key to the development of a CIRT. Nevertheless, these optional components will contribute in later phases of a CIRT.

It is also assumed that the backup server will consist of an array of Tape Storage that will follow an agreed procedure and allow for full backup and restore. The procedure will also contain processes for storing tape backup in different locations to allow for Disaster Recovery. A Disaster Recovery Proposed Network Diagram is shown in Section 4 below.

4 DISASTER RECOVERY (DR) REQUIREMENTS

In case of a failure, a disaster recovery (DR) network design has been incorporated as per the diagram below. The primary site would be the main site for running the CIRT operations while the backup site will only become active once an emergency state is declared. The DR will be a warm sites type where it will have hardware and connectivity already established, though on a smaller scale than the original production site. The warm site will have backups (tape backup) on hand, but they may not be completely updated to the DR infrastructure and may be behind by several days or a week. Manual processes for transferring the tape backups to the site will have t be incorporated to ensure that the site can be up and running in a matter of few hours. Warm Site solutions provide near-time recovery of infrastructure, data and applications through a redundant configuration. This solution is suitable for operations that can tolerate several hours of downtime while systems are updated.