FAKE Supply Chain System Project

| Team 3 Presentation|

| Fyo | Alonna | Kira | Elva |

CONTENTS

00-Background & Name
01-Purpose & Status
02-Type of Users
03-Security Architecture
04-Technical Control

00

Background & Name

00-Background & Name

Background

We has developed a Supply-chain Cloud System which is low level of sensitivity for customers located in the **Manufacturing Industry.**

Name

FAKE Supply Chain System Project

01

Purpose & Status

01-Purpose & Status

Purpose

All SCM or central planning processes created to manage an organization's demand/supply network consists of three primary activities:

Demand Management, Supply Planning or Matching Assets with Demand , Analytics Workbench.

System Status		
☐	Operational	The system is operating and in production.
☒	Under Development	The system is being **designed**, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.

02

Type of Users

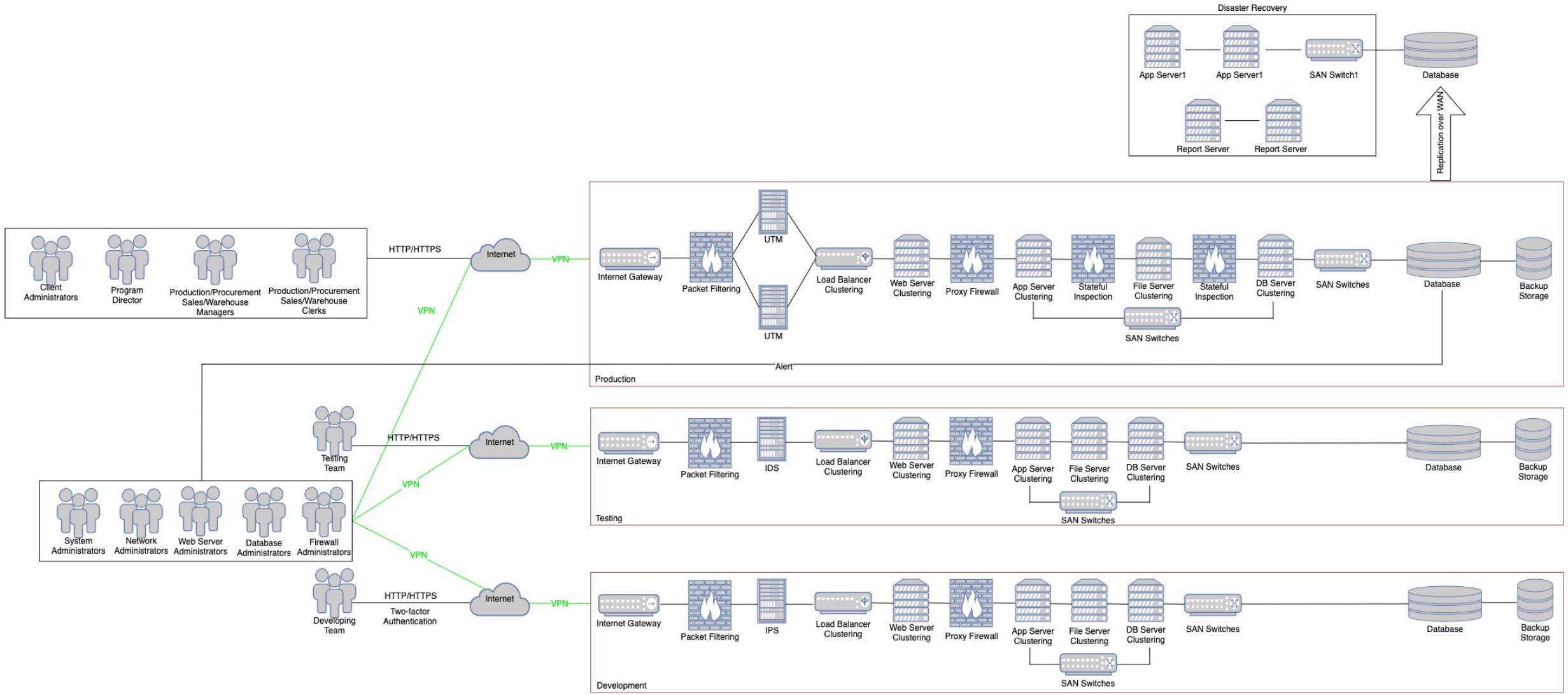
02-Type of users

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Developing team	Internal	P	High-Risk	Developing system	Develop and program the system.
Testing team	Internal	NP	Severe	Testing administration	Test the confidentiality, integrity and availability of system.
Database administrator	Internal	NP	High-Risk	Database management	Manage the databases.
Production / Procurement / Sales / warehouse managers	External	NP	Moderate	Add and approve data	Approve data from clerks and submit requirements to system administrator to change the data.
Production / Procurement / Sales / warehouse clerks	External	NP	Limited	Read and write data	Read and write data into the system.

03

Security Architecture

03-Security Architecture



04

Technical Control

04-Technical Control

ID	Control Description	Sensitivity Level Low	Solution
AU	**Audit and Accountability**		
AU-5	Response to Audit Processing Failures	AU-5	Send an alert to system administrators within 2 minutes by system.
AU-5	Response to Audit Processing Failures	AU-5	Overwrite the oldest audit records or automatically shut down; procedures should reflect escalation of priority resolution actions after 3 days.
AU-6	Audit Review, Analysis, and Reporting	AU-6	Review logs on critical systems every month. Examine logs for firewalls, routers, and other network devices which shall be time-correlated (to within 1 hour) with logs of other critical systems to determine if any incidents have occurred. Review audit logs for information systems containing PII to determine what data extracts shall be deleted monthly.
AU-6	Audit Review, Analysis, and Reporting	AU-6	Reports findings to Information Security Officers. Anomalies shall be reported in accordance with incident reporting requirements and procedures.
AU-9	Protection of Audit Information	AU-9	Rotate log files to a system other than their source system. Implement cryptographic mechanisms on information systems to protect the integrity of audit information and audit tools. Backup weekly.

THANK YOU FOR WATCHING