World Skills Competition

Trade 39:

IT PC and Network Support

Day 2 Competition

– Small Business –

Competitor Name:_____

Country Code:_____

CONTENTS

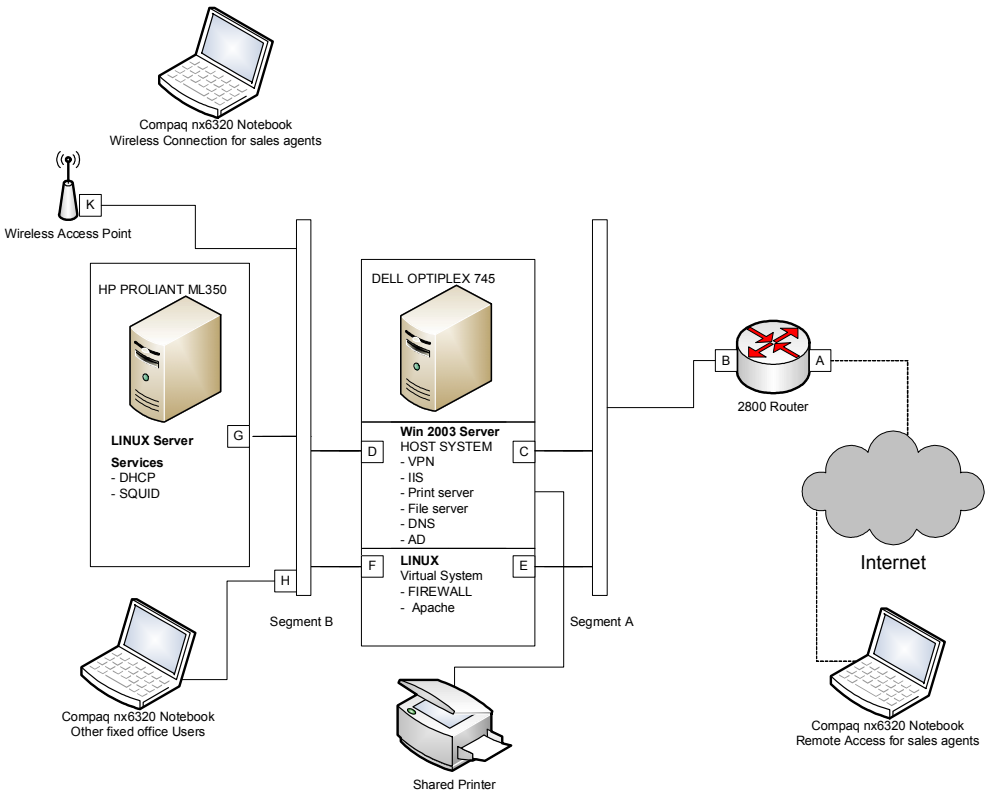
This Test Project proposal consists of the following documentation/files:

1. TP39_39Fi_day2_EN

INTRODUCTION

ExtraSafe is a small insurance company with minimal office space housing the manager, clerical support officer and system administrator. The Sales agents are flexible and operates using laptops with no fixed office space. When in the office, the sales personnel connect to the office network using the Wireless LAN. In the office, they are able to access internal files, storage, e-mail and print their documents. While on the road, the Sales personnel can connect to the office using VPN over the internet.

The logical network diagram of the office network is shown below



DESCRIPTION OF PROJECT AND TASKS

Network Description

A Cisco 2800 router with dual FastEthernet ports is used to connect to the ISP provider via a cable service (not shown). IP addresses are provided by the ISP for the connection of the router as well as for global access. In this competition you have to use the provided IP addresses shown below. To simulate the Internet Access connect the Notebook to the external port of the router.

The office network is protected from the internet by a Firewall. The Firewall is set up on the Linux server which runs as a virtual Server. The firewall will stop all unwanted incoming network traffic and allow only authorised network traffic. All internet requests from the office network must pass through the Firewall. The Apache server provides the external Website.

The office network consists of two servers. The Windows 2003 server (DELL Optiplex 745) acts as a VPN gateway, as an IIS server hosting the internal web site, and as a File-, Print and DNS server. The VPN gateway allows our Sales Agents to access the internal files and service while they are on the road. The Linux Inhouse-Server (HP Proliant ML350) provides DHCP and SQUID.

There are two types of office users. Only the manager and support pool have wired access. All other users are issued with a laptop with a wireless NIC. A wireless Access Point is used to connect these users to the office network

Main tasks:

- Configure the router
- Set up and configure Win2K3 Server
- Set up and configure the virtualized system environment (virtual pc) and use the preinstalled Linux image
- Configure all services
- Set up and configure the Linux Server
- Set up the wireless access point as well as the router

Provided IP Address

Device	**IP Address**	**Range** (last octet)	**Diagramm**
Router Fa0/0	211.10.11.1/24		A
Router Fa0/1	210.10.11.1/28		B
Physical NIC	210.10.11.2/28		C
Physical NIC	192.168.0.2/24		D
Virtual NIC	210.10.11.3/28		E
Virtual NIC	192.168.0.1/24		F
Physical NIC	192.168.0.3/24		G
Notebook (Test)	Assigned by DHCP	20 - 99	H
Wireless Access Point	192.168.0.4/255		K
Remote User Laptop	Assigned by VPN Gateway	100 - 150	
DHCP Server on the Router	211.10.11.x	100 - 150	

- **Windows 2003 Server**

The Windows Server is a dual homed PC running Windows 2003 SP2

Main Services

- VPN Gateway
- IIS
- Print Server
- File Server
- DNS
- Active Directory

Server

This system has 1 hard disk. Install Windows 2003 Server operating system. Create 3 partitions. One for the Windows System (SYSTEM), one for the Virtual Server (VS) and one for the File sharing (FS). Use for the System a 20GB partition, for the virtual Server also a 20GB partition and use the rest of the HD space for filesharing. Ensure that all partitions are formatted using NTFS.

The server is named Win2K3VPN. Set the organisation name to ExtraSafe and use the default parameters. Install AD. Use extrasafe.com as Domain name. Use the default parameters.

After installation, create a new Administrator account shown in the table below. Rename the Administrator account to "localuser".

Each user will be limited to 500 MB of disk space. In the event when a user exceeds his quota, the event will be logged. Enable a user warning when user reach 450MB

The home directory for all users is on the 3rd partition (FS) in the folder HOME. The folder for sharing documents is also on the 3rd partition named SHARE. Ensure that all shared folders are not visible.

The accounts on the server are as follows:

Account	Group	Password
Localuser (Administrator)	Administrators	123456
Bigboss	Administrators	123456
Manager	Administrators	123456
Support	Power User	123456
Salesagent001	Sales Agent	123456
...	...	123456
Salesagent100	Sales Agent	123456

The password for the Sales Agents has to be changed on 1st login by the user. Users have only 3 chances to login in. Un-successful logins are logged and the user is locked out for 15 minutes. You will need to write a script to generate the salesagent accounts. Store the script on the desktop of the User „bigboss“. If you want to test the login for the sales agents use the user salesagent001 to salesagent050.
[NOTE: For marking reasons you are not allowed to use salesagent051 to salesagent100]

Support on the Win2K3 server is important. Hence, you are to allow ONLY members of the Administrators group to access the server via terminal services. You can test this using the laptop provided.

A Printer is provided for the office users. Install and share this printer for the office.

IIS

Install IIS and enable the Web server but disable the FTP server. Configure the server to allow Anonymous Authentication Access. For performance reasons, limit the number of concurrent connections to 50 and limit the bandwidth available for connections to 4 Mb/s. Prevent the webserver from consuming too much processor time by limiting the CPU usage to 20%. Copy the provided HTML File (internal.html) as default HTML Page to the folder.

The server also provides Certificate Services for authentication of the HTTP server. Use the following information to configure this service.

CA Name	ExtraSafe_Certificate_Server
Organisation	Extra Safe Insurance Services
Organisation Unit	ES_IS
City	Tokyo
CA Description	Certificate for ExtraSafe
Valid for	1 Year

You should use the default settings for the data storage location when configuring the Certificate Server. You have to enable SSL for all users who interact with the web site. Install a certificate from the CA Server when configuring IIS. Provide your own information when requesting the certificate.

This web page is only accessible to internal users. Deny all external users from accessing this page. This page is accessible by intranet.extrasafe.com

VPN

Sales personnel who are outside the office, can access internal network services by using VPN. Configure the Win2K3VPN server to accept incoming VPN via the internet. The VPN gateway will assign the necessary internal IP addresses to incoming users. You are also required to configure your laptop as a VPN client. You have to deny all other traffic from the external interface.

- **LINUX Firewall**

This is a virtual dual homed PC. The Firewall blocks all incoming/outgoing network traffic except DNS and HTTP / HTTPS.
Install Virtual PC on the specified partition (VS) and copy the source image on it. The root Password is “extrasafe”. Please don’t change the root password; otherwise we can not mark your work.

Enable SSH services for internal remote logins, however, disable the remote root login. You should also disable and un-install the Telnet client and server if necessary. eth0 [E] connects to the external network, while eth1 [F] connects to the internal network. Disable all non-essential services on the firewall and only allow incoming/outgoing DNS, HTTP and HTTPS network traffic from the SQUID Server.

Create a user “bigboss” with the password 123456
This Account will be used as SSH administrator.

The Firewall provides HTTP and HTTPS services only for the Internet users. Use the provided WebPages [external.html] for HTTP as default page and [external_https.html] for HTTPS as default page.

Enable NAT Services for this system.

- **Linux Server**

The Linux Server provides the necessary DHCP and SQUID service.

Install Linux on the HP Proliant ML350 Server. Set up a RAID 5 System Disc. Create 2 partitions

/ : 210GB.

swap : the Rest of the space

Name your server "Linux-Server". Select the default install of the server. Use the password 123456 for the root account. Create the account „bigboss“ with the Password 123456

All information should be provided from the proxy server. Use port 8080 / all access permitted. Sales agents who connect to the network are automatically assigned an IP address. Install squid. Any user from the internal network who wishes to access external internet pages should go through this proxy. No internal user should be able to access the internet directly. Stop all other services.

NOTE: If you have problems during the installation the provided paper sheet can help.

- **Wireless Access Point**

The CISCO Access Point connects the Sales personnel to the office network.

Connect the Wireless Access Point to the internal office network. Setup the Access Point to have a SSID of "StationNN" where NN is your station number. (For example station number 5 is 05) Do not broadcast your SSID. For security purposes, setup 40-bit WEP using the following code: NN01020304 where NN is your station number. You have to configure your laptop using the wireless NIC for connectivity to the network. Users from within the network are able to access all internal network services. The wireless Access Point should have a designated name of "StationNN" where NN is your station number. Set the MAC Address filtering. Only the Notebook provided should connect to the Access Point. Reduce the transmitter-power to 1mW. Do not change the default password of the Wireless Access Point.

- **Network**

Set up the network comprising of the Router, Linux Firewall, Windows 2003 Server and Wireless Access Point. Use the external cable to test your VPN Gateway. The public IP Address is provided by the Router.

Cisco 2960 Switch

2 managed switchs are provided for you to use.

Cisco 2800 Router

Use static routes for your router. Name your router ,"RouterNN" where NN is your Station Number (e.g. Station 5 = Router05). Do not enable any password for the router. This Router provides DHCP services for external users..

- **Client Notebook**

A preinstalled Client Notebook is provided for wired and wireless testing witch includes tests for the internal and external network.

- **Printing**
  - Print out the Access Point configuration
  - Print out the Router configuration
  - Print out the iptables
  - Print out the Script how generate the salesagent accounts