Test Project – Day 4

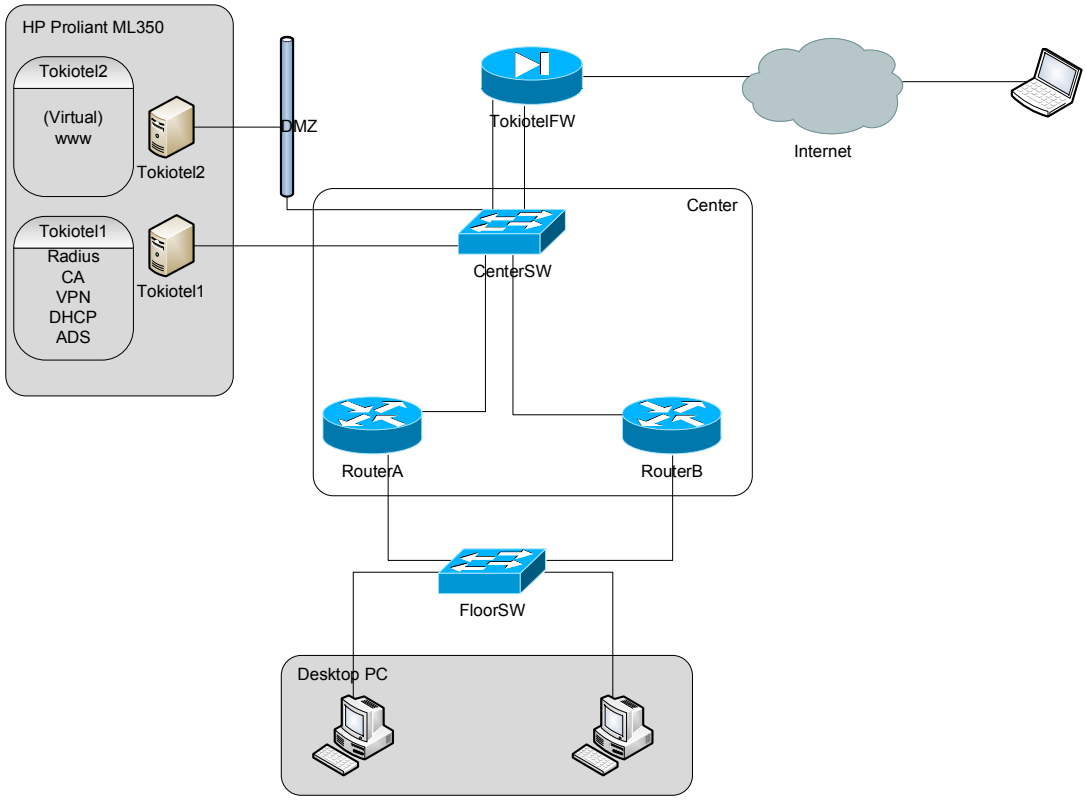
TP39_39JP_EN_v1.4

INTRODUCTION

- The competition has a fixed start and finish time. You must decide how best divide your time.

You can decide which task to begin with.

Project description and tasks



SCENARIO

You work for Information System department in TokioTEL corp. The company distributes kiosk-computer solutions to coffee shops, shopping centre and other stores. The kiosk-computers need to connect LAN in the headquarters via internet VPN.

The company board of directors decided to enhance a company system security and its availability, and appointed you as a project manager.

DESCRIPTION

All network equipment will be **rebooted** before marking!

Network

Desktop PC can be connected to 2 VLANs (VLAN20 and 30) and its allocated IP addresses by DHCP. For a gateway fault, all gateway devices must be redundancy and other gateway devices can perform as the gateway using 2 VLANs at regular process in order to spread its workload.

For network security, FW stores internet lines. The company has one webserver in a DMZ that provides www services to internet.

Internal Server

There is a Windows 2003 server acting as a domain controller placed in the headquarters. Kiosk-computers placed in various stores will log on this server via internet VPN. RADIUS installed in this server authorizes network devices. This server also provides DNS and DHCP services.

External Server

There is a virtual Windows 2003 server providing www services to public Internet.

SPECIFICATIONS

Network

Use the following VLAN numbers:

VLAN 10 Center

VLAN 11 DMZ

VLAN 20 GroupA

VLAN 30 GroupB

Set IP address (see table A on appendix) and hostname (see table B on appendix).

In case that either router breaks down, you need to secure the communication using VLAN 10, 20 and 30 to other segment. VLAN 20 uses Router A, and VLAN 30 uses Router B preferentially. However, if router breaks down, they are considered as fault devices. In such case, use other devices.

Router setting

Set “Enable Secret Password” to “Admin”.

Require Radius authentication for Console and Telnet connection. If failed, local authentication is required:

Radius accounting: see server side setting

Shared key is the routers hostname

Local account: User name is Admin, password is Admin.

Set appropriate static routing for the provided topology.

Set all network devices enabling secure redundancy and workload spread as specified.

Set physical connection as below:

RouterA

Connect Fa0/0 to Fa0/6 in FloorSW, and Fa0/1 to Fa0/6 in CenterSW.

RouterB

Connect Fa0/0 to Fa0/7 in FloorSW, and Fa0/1 to Fa0/7 in CenterSW.

Switch common settings

Create necessary VLANs.

Set “Enable Secret Password” to “Admin”.

Require Radius authentication for Console and Telnet connection. If failed, local authentication is required:

Radius accounting: see server side setting

Shared key is the switchs hostname

Local account: User name is Admin, password is Admin

Switch A (FloorSW) settings

Set interface Fa0/2 for VLAN20, Fa0/3 for VLAN30. Do not use any other ports.

Set Fa0/02 and Fa0/3 disabling them to connect to any PC other than desktop PC.

Link up Fa0/2 and Fa0/3 by shortening spanning tree calculation.

Set port Fa0/2 100Mbps speed and full duplex.

Switch B (CenterSW) settings

Connect FW, RouterA, RouterB and Windows servers.

Set interface Fa0/4, Fa0/5, Fa0/6 and Fa0/7 for VLAN10.

Set interface Fa0/2 and Fa0/3 for VLAN11.

Firewall (TokiotelFW) settings

Set “Enable Password” to “Admin”.

Require Radius authentication for Console and Telnet connection. If failed, local authentication is required:

Radius accounting: see server side setting

Shared key is the firewalls hostname

Local account: User name is Admin, password is Admin

Set a static routing. Establish a default route for the internet and a route for the internal network.

Physical connection

Connect interface “Internal/Ethernet 1” to Fa0/3 in CenterSW, and “External/Ethernet 0” to the notebook that simulates the Internet.

Filtering settings

Limit access between internal and external network based on the following policy:

External → Internal
Allow VPN. Prohibit any other connections.

External → DMZ
Allow HTTP. Prohibit any other connections.

Internal -> External
Allow all connections other than IRC, TELNET, P2P and FTP connections. However, only P2Pport 1337/tcp, 1214/tcp, 4661-4672/tcp.6881-6889/tcp.

Port forwarding settings

Forward external VPN connections from Internet to Tokiotel1.

Forward external HTTP connections from Internet to Tokiotel2.

Forward internal HTTP connections from internal network to Tokiotel2.

Use standard port numbers.

HP Proliant ML350 (Tokiotel1) settings

You need to enable the BIOS-setting “Intel Virtualization Technology” on the HP Proliant ML350 to be able to install 64 bit operating system in VMWare.

Physical connection

Connect the servers onboard network card to Fa0/4 in CenterSW.

OS settings

Set up Active Directory on the server and create an Organizational Unit and user accounting referring to table C on the appendix. Each user account has to provide remote access for the user.

Create a security template in accordance with the following requirements:
Security template: skill39
Password can change at least every 5 days and is valid for 30 days. Password must have at least 5 characters and the last 5 used passwords do not work. After 5 incorrect logins, the account will be deactivated for 10 minutes.

DHCP

Set up DHCP service in order to allocate IP-addresses to GroupA and GroupB. IP-address lease time is 2 days. Set up necessary options allowing each client to log on the domain. Set up options as required.

VPN

Set up VPN connection (L2TP/IPSec) on the server enabling Kiosk-computers to connect to the headquarters’ LAN via internet VPN.

VPN access to tokiotel1 server is accepted only with L2TP/IPSec (PPTP connection isn’t allowed). Allow access from L2TP/IPSec only up to 10 times.

Computer certification for IPSec is to be used as mentioned later. Refer to CA section for certificate authority.

RADIUS

Install RADIUS server functions onto tokiotel1 server. Use each equipment hostname as shared secret (RADIUS key).

Group policy

Set the group policy in accordance with the following requirements:

Policy: Kiosk-pol

Set Kiosk OU in accordance with the following requirements:

Set the Internet Explorers default page to http://tokiotel.skill39.local. The default page is not changeable.

The only applications users can use are Internet Explorer and notepad.

Remove link and access to Windows Update.

Remove programs in the settings menu.

Do not save desktop settings at the end of users session.

Remove “trash” icon from the desktop.

CA

Set up Enterprise certificate authority in tokiotel server. CA common name is “tokiotelCA”. Set Default Domain Policy to distribute the computer certification automatically.

HP Proliant ML350, virtual server (Tokiotel2) settings

Create a suitable virtual machine on VMWare server and connect it’s NIC to the HP Proliant ML350 servers non-onboard NIC.

OS setting

Refer to the appendix (virtual server specifications) for setting requirements.

Physical connection

Connect the server to Fa0/2 in CenterSW.

IIS

Install IIS and edit Web starting page to display your stations number. Each PC should be able to access the Web site with http://tokiotel.skill39.local

Notebook (Kiosk-pc) settings

Refer to the appendix (notebook specifications) for setting requirements.

Create a VPN connection to Tokiotel1.

Encrypt connection with Tokiotel1 using IPSec. Use the computer certification for IPSec authentication. Refer to the previous CA section for CA settings.

Desktop PC (Floor-pc) settings

Refer to the appendix (desktop PC specifications) for setting requirements.

APPENDIX

Table A

No	Subnet	Address
I	DMZ	205.157.3.0/26 TokiotelFW: 205.157.3.62
II	GroupA	172.16.20.0/24 FloorSW: 172.16..20.200
III	GroupB	172.16.30.0/24
IV	Center	172.16.11.0/24 TokiotelFW 172.16.11.250 CenterSW: 172.16.11.200
V	FW ~ ISP	210.148.x.0/29 TokiotelFW 210.148.x.6, ISP-Router 210.148.x.1

Gateway address in each segment is to use the last address in the segment. If you use more than one router on the same subnet, set the last address minus 1 as RouterA, minus 2 as RouterB.

Every subnet which uses dynamic IP should address hosts from the 4th octet number (1 to 99).

If there is an x letter in a IP address you should replace it with your stations number.

Table B

No	Hostname	Device
I	RouterA	Router A, Cisco 2811 router
II	RouterB	Router A, Cisco 2811 router
III	FloorSW	Switch A, Cisco Catalyst 2960G switch
IV	CenterSW	Switch A, Cisco Catalyst 2960G switch
V	TokiotelFW	Firewall, Cisco PIX 515E
VI	Tokiotel1	HP Proliant ML350
VII	Tokiotel2	Virtual machine in HP Proliant ML350
VIII	Kiosk-pc	Notebook, HP Compaq nx6320
IX	Floor-pc	Desktop PC, Dell Optilplex n

Server specifications

Operating system: Windows 2003 server R2 SP2

Hostname: Tokiotel1

Domain name: skill39.local

Administrator password: Admin

IP address: 172.16.11.151/24

Table C

No	User name	Password	Organization Unit or Container	Remarks
1	kiosk-u001	Admin	KIOSK	kiosk-u001authorize only logon by kiosk-pc user account for Kiosk-pc
2	Floor-u001	Admin	Users	Use for PC connecting to internal LAN
3	Net-u001	Admin	Users	Authentication account for network devices

* Provide remote access permission to each user as needed.

Virtual server specifications

Operating system: Windows 2003 server R2 SP2

Company name: Tokio Tel Inc

Organization name: Tokio Tel Inc

Hostname: Tokiotel2

Workgroup: Workgroup

Administrator password: Admin

IP address: 205.157.3.51/26

Notebook specifications

Operating system: Windows XP professional SP2

Hostname: Kiosk-pc

Domain name: skill39.local

Administrator password: Admin

IP address: 210.148.x.4/24

Desktop specifications

Operating system: Windows XP professional SP2

Hostname: Floor-pc

Domain name: skill39.local

Administrator password: Admin

IP address is automatically assigned when PC3 connects to FloorSW.

Instructions to the competitor

Do not bring any material with you to the competition.

Mobile phones are not to be used.

The competition has been designed to give you too much to do in the time.

Do not disclose any competition material/information to any person during each day's competition.

Read the whole competition script prior to you starting work.

Be aware that different tasks attract a percentage of the overall mark. Plan your time carefully.

Any technical problems must be reported immediately. Equipment will be checked and if found faulty will be replaced and extra time will be agreed with the competitor. However if the equipment is found to be working correctly, no extra time will be given.

You may ask questions during the competition to judges who will always work in pairs; however the judges reserve the right not to answer. All answers given will be written down and where appropriate given to all other competitors.

Equipment, machinery, installations and materials required

1. VMWare CD
2. CD with jdk

Marking scheme

Marking schemes will only be provided at the start of the competition.