Island D – Test Project – Integration and Network Security

WSC2013_TP39_ISLAND_D_actual_EN

Submitted by:
José Medeiros PT
Franz Winkler AT
Wayne Second TT
Olli Janatuinen FI
Jit How Hwang SG
Te Chao Liang TW
Kevin Large UK

OVERVIEW

MODULE – ISLAND D

CONTENTS

This Test Project proposal consists of the following document/file:

1. WSC2013_TP39_ISLAND_D_actual_EN

INTRODUCTION

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

DESCRIPTION OF PROJECT AND TASKS

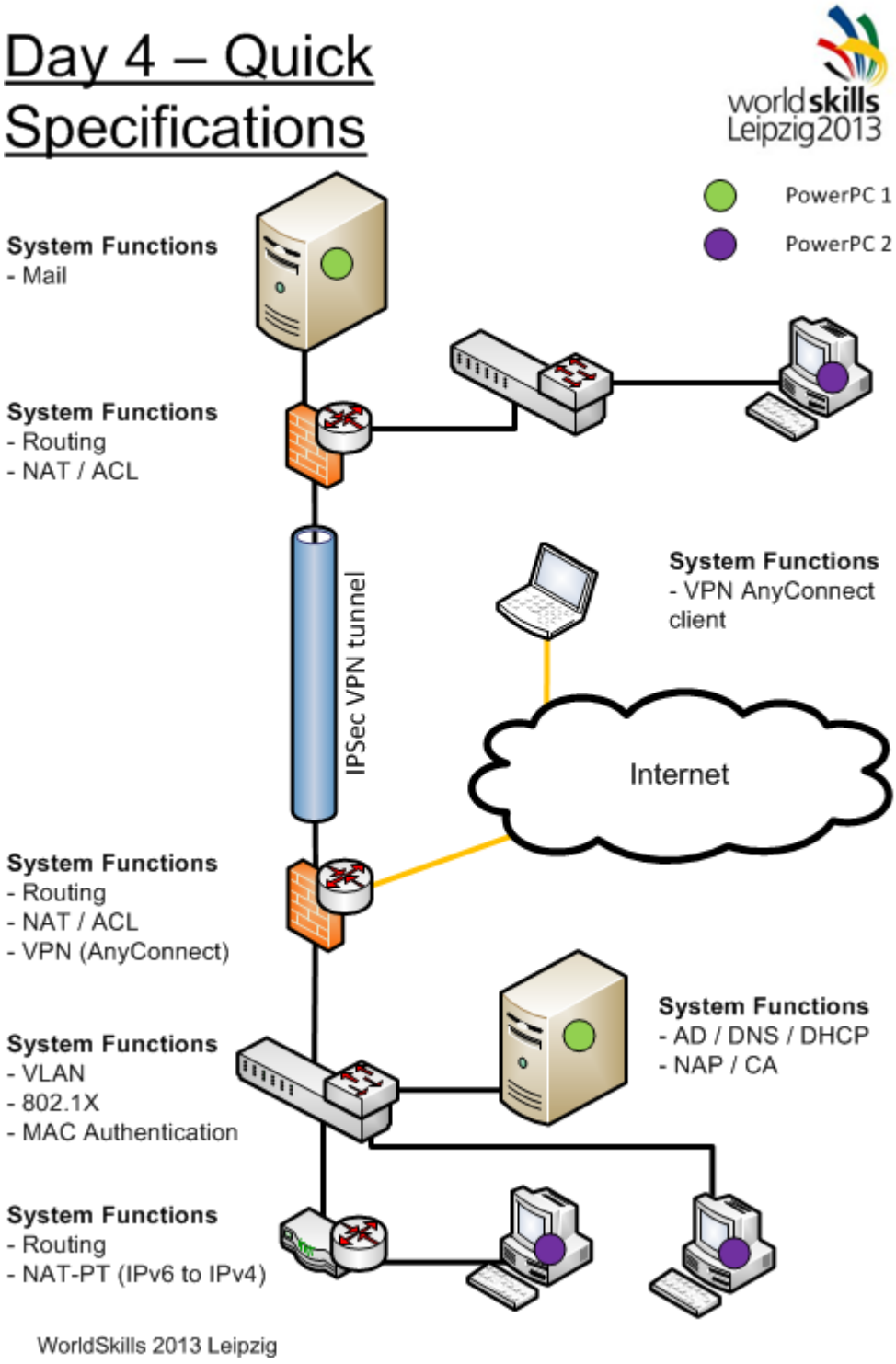
You are working for a research company.
The management assigned you with the integration of a datacenter site as well as the securing of the existing network infrastructure.
The headquarters and the datacenter should be connected through a secure IPSec VPN tunnel.
The datacenter is used for services accessible from internet, like the company's mail system.
A windows client for management reasons is located in the inside network of the datacenter.
In the headquarters, you have decided to use several security mechanisms to ensure access is given only to computers of the company.
Further, the laboratory network with linux clients is separated from the inside network by a router.
Remote access should be given to managers and consultants using Cisco's AnyConnect VPN solution.
Additional information is provided in the appendix.

Notes:

1. The password for everything is: **Skills39**

2. Base VMs have been provided. You are free to use them or install from scratch. All the software is located in drive D in the Leipzig2013 folder.

QUICK SPECIFICATIONS



PART 1

Work Task Server winsrv1
Note: Please use the default configuration if you are not given the details.

- Configure the server with the settings specified in the appendix
- Install the services
  - Active Directory
    - Use “research.local’ as domain name and RESEARCH as NetBios name
    - Create the users and groups specified in the appendix
  - DNS
    - Install DNS services
  - DHCP
    - Range: 172.16.129.0 – 172.16.129.199
    - Gateway: 172.16.128.1
    - Primary DNS: 172.16.128.10
    - DNS-Suffix: research.local
  - NAP for 802.1x
    - Make sure only Domain Computers are allowed
    - Use computer account based authentication with certificates
    - Put healthy clients into VLAN100
    - Put unhealthy / non-compliant clients into VLAN999
    - Disable automatic remediation of unhealthy clients
  - CA
    - Install CA services
    - Create root CA certificate
    - Add CA on all domain computers as trusted root CA
  - NTP
  - Install and configure this machine as a NTP server
    - NTP clients are: hqrtr1, hqswi1 and hqsec1

Work Task Server lnxsrv1
Note: Please use the default configuration if you are not given the details.

- Set up the servers with the operating system (Debian 6). Ensure that all components are correctly installed
- Configure the server with the settings specified in the appendix
- Install the services:
  - Mail
    - Create users peter and mary
    - Make sure they have access via POP3S, IMAPS and SMTPS
    - Enable web access over HTTPS
    - Use certificates signed by winsrv1 for SSL/TLS encryption or use self-signed certificates
    - Before you finish your project make sure you send an email message from peter to mary and another message from mary to peter.
    - Do not delete these email messages.

- Install and configure a syslog server
  - hqsec1, dcsec1 and dcswi1 should send logs to the syslog server.
  - Set the logging level at informational

PART 2

Work Task Network hqrtr1
Note: Please use the default configuration if you are not given the details.

- Connect LAN cables and configure IP addresses according to the network diagram in the appendix
  - G0/0: hqswi1
  - G0/1: lnxclt1

- Configure routing
- Configure NAT-PT
    - Make sure all clients of laboratory network (IPv6-only) can access winsrv1 (IPv4-only)
    - winsrv1 should be reachable from IPv6-network using address 2001:12::ac10:800a
    - Configure dynamic address mapping
    - Use addresses 172.16.129.200 – 172.16.129.249 on IPv4-side
- Remote access, for the purpose of management, should be restricted to SSH.
    - Remote access user id: **remote** Password: **Skills39**

Work Task Network hqswi1

Note: Please use the default configuration if you are not given the details.

- Connect LAN cables and configure IP addresses according to the network diagram in the appendix
    - Port 1: hqsec1
    - Port 2: hqrtr1
    - Port 3: winsrv1
    - Port 4: winclt2
    - All other ports should be configured for clients
- Use as default the VLAN100
- Make sure only winclt2 and the VM host mac address are allowed to communicate through port 4
    - Use MAC authentication
    - In case of violation, the port should be set to “shutdown”
    - Configure automatic recovery after 30 seconds
- Configure port security on port 24
    - Maximum 1
    - Static MAC address is E8-03-9A-F7-39-9D
    - In case of violation, the port should be set to “shutdown”
- Configure DHCP snooping
    - Allow only the winsrv1 DHCP server
- Use 802.1x authentication for all client ports from f0/5 to f0/22
    - Make sure only clients approved by winsrv1 are allowed to communicate
    - Use VLAN information provided by winsrv1
- Remote access, for the purpose of management, should be restricted to SSH.
    - Remote access user id: **remote** Password: **Skills39**
- Configure portfast on all access ports

Work Task Network hqsec1

Note: Please use the default configuration if you are not given the details.

- Connect LAN cables and configure IP addresses according to the network diagram in the appendix
    - Port 0: dcsec1
    - Port 1: winclt1
    - Port 2: hqswi1
- Configure routing
- Configure IPsec VPN tunnel
    - Use certificate signed by CA on winsrv1, self-signed certificate or pre-shared key for authentication
    - Use AES-256 for encryption and SHA for integrity.
- Configure source NAT for internet access
- Configure AnyConnect VPN
    - Use address range 10.0.0.0 – 10.0.0.100 /24
    - Allow access only to winsrv1 and lnxsrv1
    - Configure split-tunneling
        - Only route traffic to winsrv1 and lnxsrv1 through VPN tunnel
    - Make sure VPN software does not remain on client after connection is closed

- Configure the firewall as restrictive as possible, keeping in mind that “permit ip any any” is not allowed, but allow for all services requested in the Test Project.
    - Allow ping to and from every interface.
    - Allow ping between winsrv1 and dcswi1 and vice-versa
- Configure SSH to allow connections from the Internet

Work Task Network dcsec1
Note: Please use the default configuration if you are not given the details.

- Connect LAN cables and configure IP addresses according to the network diagram in the appendix
    - Port 0: hqsec1
    - Port 1: lnxsrv1
    - Port 2: dcswi1
- Configure routing
- Configure IPsec VPN tunnel
    - Use certificate signed by CA on winsrv1, self-signed certificate or pre-shared key for authentication
    - Use AES-256 for encryption and SHA for integrity.
- Configure security levels
    - 0 for outside
    - 50 for DMZ
    - 100 for inside
- Configure source NAT for internet access
- Make sure mail services (SMTPS, POP3S, IMAPS, Web via HTTPS) are accessible from internet
- Configure the firewall as restrictive as possible, keeping in mind that “permit ip any any” is not allowed, but allow for all services requested in the Test Project.
    - Allow ping to and from every interface.

Work Task Network dcswi1
Note: Please use the default configuration if you are not given the details.

- Connect LAN cables and configure IP addresses according to the network diagram in the appendix
    - Port 1: dcsec1
    - Port 2: winclt3
    - All other ports should be configured for clients
- Remote access, for the purpose of management, should be restricted to SSH.
    - Remote access user id: **remote** Password: **Skills39**
- Configure portfast on all access ports

PART 3

Work Task winclt1
Note: Please use the default configuration if you are not given the details.

- Configure the client with the settings specified in the appendix
- Create a shortcut to webmail (lnxsrv1) on Desktop
- Configure the email client:
- Configure an account for user peter with protocols SMTPS and POP3S
- Configure an account for user mary with protocols SMTPS and IMAPS
- Send mail from one user to the other and vice-versa
- Send mail from each user to himself
- DO NOT DELETE the email messages

Work Task winclt2
Note: Please use the default configuration if you are not given the details.

- Configure the client with the settings specified in the appendix
- Configure 802.1x / NAP
    - Make sure the server certificate is being checked

- Join client into domain “research.local”

Work Task winclt3
Note: Please use the default configuration if you are not given the details.
- Configure the client with the settings specified in the appendix

Work Task lnxclt1
Note: Please use the default configuration if you are not given the details.
- Set up the client with the operating system (Debian 6). Ensure that all components are correctly installed
- Install a GUI (graphical user interface) of your choice
- Configure the client with the settings specified in the appendix
- Create a shortcut for the share NETLOGON (winsrv1) on the Desktop

APPENDIX

SPECIFICATIONS

ACTIVE DIRECTORY USERS

Account	Group	Password
Local user (Administrator)	Administrators	Skills39
User01	Office	Skills39
…	…	Skills39
User99	Office	Skills39
Researcher01	Laboratory	Skills39

winsrv1

Organization:	research
Computer name:	winsrv1
Domain name:	research.local
User name:	Administrator
Administrator password:	Skills39
IP addresses:	172.16.128.10

lnxsrv1

Organization:	research
Computer name:	lnxsrv1
Domain name:	research.local
User name:	root
Administrator password:	Skills39
IP addresses:	192.168.10.2

winclt1

Organization:	research
Computer name:	winclt1
Domain name:	research.local
User name:	Administrator
Administrator password:	Skills39
IP addresses:	81.6.63.115

winclt2

Organization:	research
Computer name:	winclt2
Domain name:	research.local
User name:	Administrator
Administrator password:	Skills39

IP addresses:	DHCP

winclt3

Organization:	research
Computer name:	winclt3
Domain name:	research.local
User name:	Administrator
Administrator password:	Skills39
IP addresses:	192.168.20.10

lnxclt1

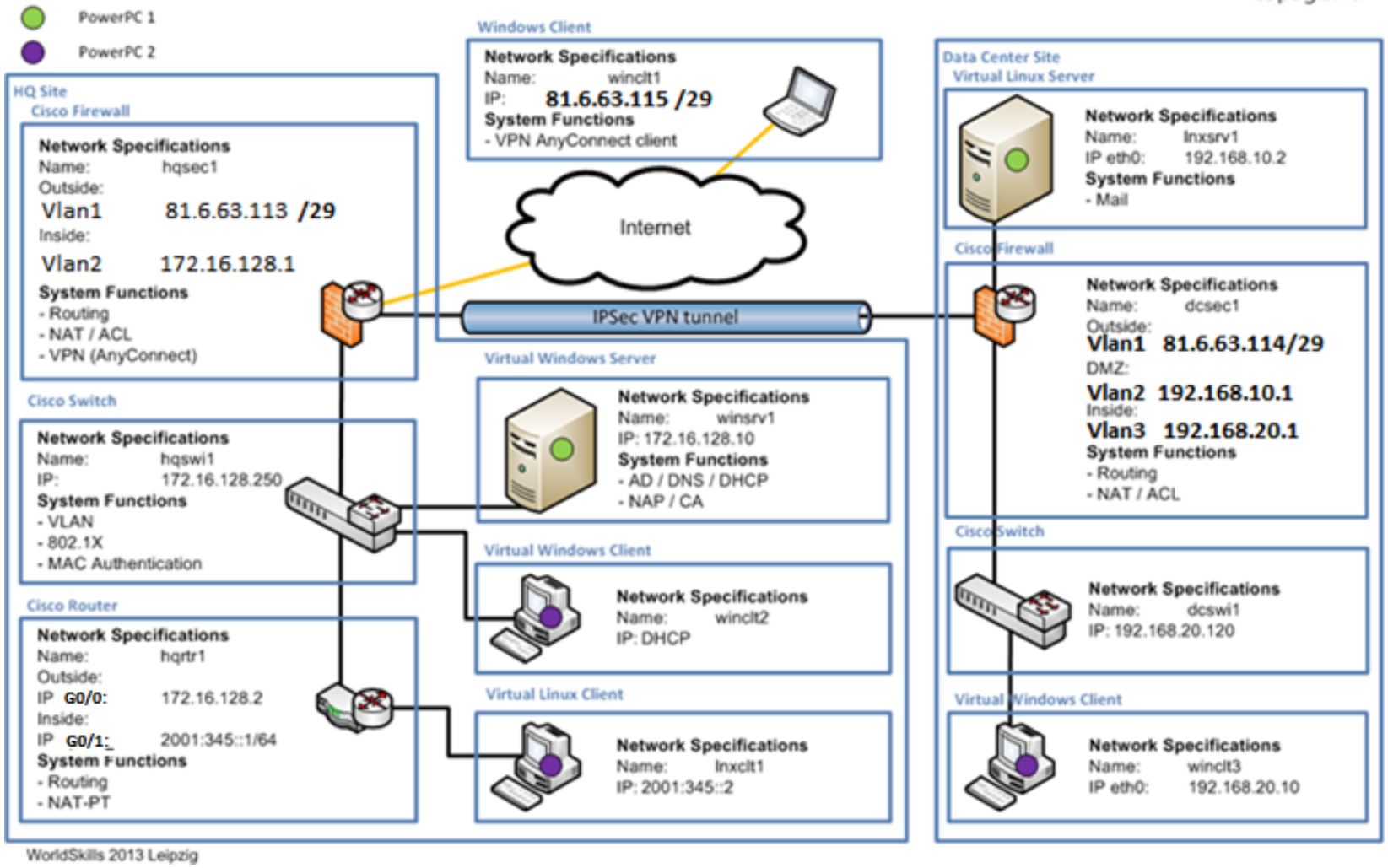
Organization:	research
Computer name:	lnxclt1
Domain name:	research.local
User name:	root
Administrator password:	Skills39
IP addresses:	2001:345::2

NETWORK SPECIFICATIONS

External network	81.6.63.112 /29
HQ VLAN 100 (default)	172.16.128.0/23
HQ VLAN 999 (isolated)	-
HQ Laboratory	2001:345::/64
DC DMZ	192.168.10.0 /28
DC Inside	192.168.20.0 /25
Enable password cisco devices	Skills39

NETWORK DIAGRAM

Day 4 – Integration and Network Security



INSTRUCTIONS

INSTRUCTIONS TO THE COMPENTITOR

- Do not bring any materials with you to the competition.
- Mobile phones are not to be used.
- Do not disclose any competition material / information to any person during each day's competition.
- Read the whole competition script prior to starting your work.
- Be aware of different tasks attract a percentage of the overall mark. Plan your time carefully.

EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

PowerPC 1:

- Performance PC with 8Gb memory with 2 network cards
- VMware Workstation preinstalled
- VMs are preconfigured
- winsrv1
  - 1x Disk 40GB
  - 4GB memory
  - 1 CPU
  - 1 network card in bridged mode (LAN)
  - OS preinstalled (Windows Server 2008 R2)
- lnxsrv1
  - 1x Disk 10GB
  - 2GB memory
  - 1 CPU
  - 1 network card in bridged mode (LAN)

PowerPC 2:

- Performance PC with 8Gb memory with 3 network cards
- VMware Workstation preinstalled
- VMs are preconfigured
- VMs OS is preinstalled (Windows 7)
- winclt2, winclt3
  - 1x Disk 40GB
  - 3GB memory
  - 1 CPU
  - 1 network card in bridged mode (LAN)
  - OS preinstalled (Windows 7)
- lnxclt1
  - 1x Disk 10GB
  - 1GB memory
  - 1 CPU
  - 1 network card in bridged mode (LAN)

Laptop:

- Laptop without WiFi and Bluetooth
- OS preinstalled (Windows 7)

Network:

- 2x Switch Cisco 2960
- 2x Firewall Cisco ASA 5505
- 1x Router Cisco 1941 - SEC/K9 (IOS UNIVERSAL - S190UK9-15104M)

Additional software:

- Operating System (Windows 7)
- Operating System (Windows Server 2008 R2)
- Operating System (Debian 6) (DVD1-8)
- Drivers for peripherals

Additional equipment: None