TEST PROJECT IT NETWORK SYSTEM ADMINISTRATION

MODULE B – WINDOWS ENVIRONMENT

WSC2017_TP39_ModuleB_actual

Submitted by:
Stefan Wachter LI
Mohamad Ropi Abdullah MY
Silvio Papić HR
Doug Warden CA
Roger Sánchez ES
Svetlana Lapenko KZ
Alan Au MO
Joe Motsapi ZA
Hamed Kargarzdeh IR

1. INTRODUCTION TO TEST PROJECT DOCUMENTATION

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

2. CONTENTS

This Test Project consists of the following document/file:
WSC2017_TP39_Module_B_EN_v1.0.docx (This document)

- Excel file for the user import (RU-Users.xlsx)
- Websites for install
    - Manager Website
    - www.RUSSIA.net Website
- RSAT Tools (WindowsTH-RSAT_WS2016-x64.msu)
- Windows 10 ADMX files (Windows_ 10_Creators_Update_ADMX.msi)
- Windows Server 2016 ISO

3. DESCRIPTION OF PROJECT AND TASKS

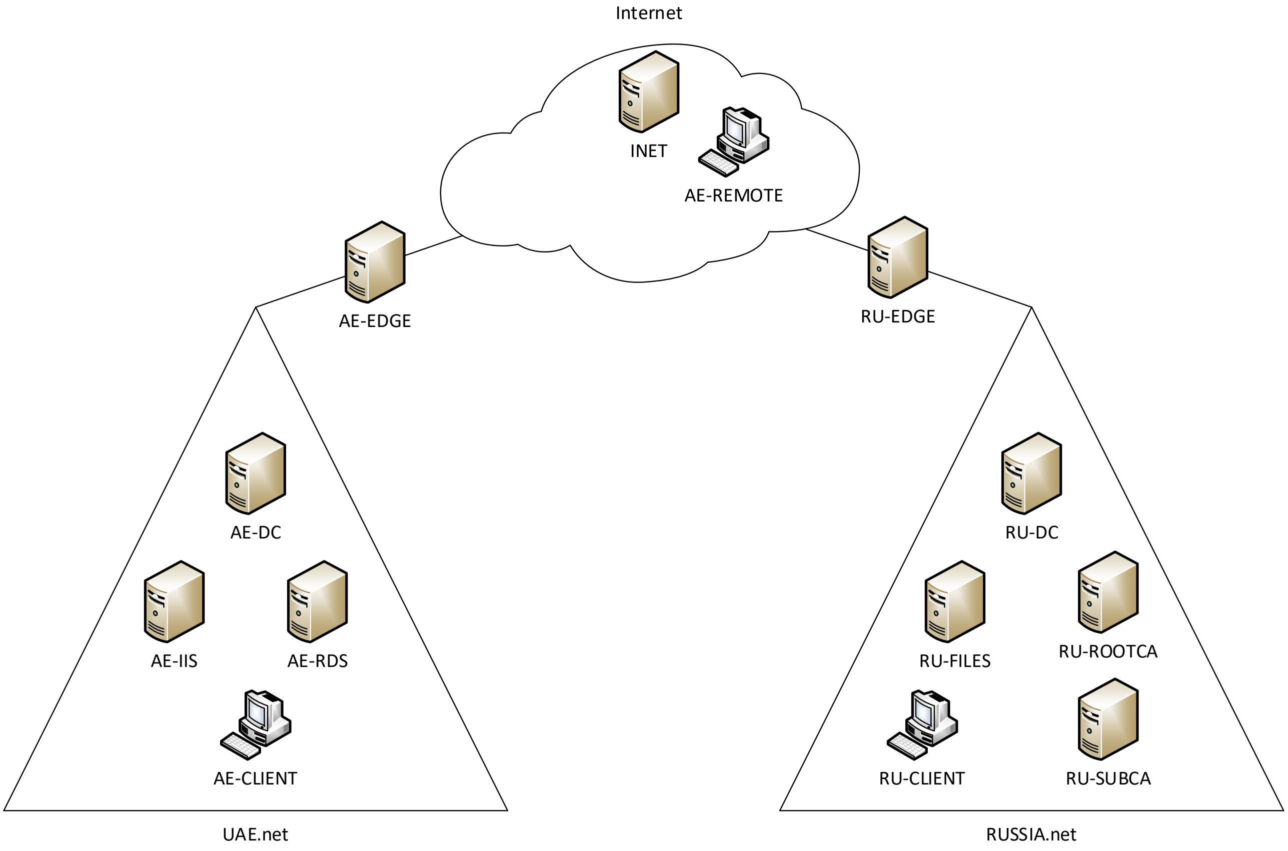
Introduction

You are the IT consultant responsible for Skill39 in Abu Dhabi. There is already an existing domain UAE.net. You have to build and configure the network for the next WorldSkills competition in Kazan, which consists of a new domain RUSSIA.net and copy some of the users to this new domain and also implement features for external access to the network, policies and file services.
This project several components, you need to:

1. Build a new domain (RUSSIA.net) which will eventually host all the users and computers for the next competition
2. Maintain connectivity and access to resources between the new domain and the old domain (UAE.net) while the transition is being made
3. Copy some of the users and data from the old domain to the new one

~~4.~~ Setup a new site-to-site connection

Quick Specifications



Part 1 – RUSSIA.net

In Part 1 you will be responsible for preparing the new domain prior to performing the migration. This will involve building the RUSSIA.net domain, including all of the resources that will be necessary for the future migration, preparing for secure connectivity between the new domain and the old domain - which will involve setting up a VPN server and a multi-tier PKI infrastructure.

NOTE: Refer to the diagram on the last page for quick specification reference, as well as the configuration table.
Please use the default configuration if you are not given the details
All local and domain users on ALL machines should have a password of "P@ssw0rd" unless otherwise specified. Pre-supplied machines that the competitor needs to logon to will also be pre-configured with this password.
All supplied software and files needed to complete this project can be found in C:\software on the competitor computer.

Work Task RU-DC

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic

Active Directory

- Configure this server as the initial domain controller for RUSSIA.net
- Configure an ONE-WAY (Forest) trust between the domains RUSSIA.net and UAE.net
  - Users from RUSSIA.net must have access to resources from UAE.net but not vice versa

DHCP

- Configure DHCP for the clients
- Mode: Load balancer
- Partner Server: RU-FILES
- State Switchover: 10 minutes
- Range 172.16.0.150-180
- Set the appropriate scope options for both DNS servers and default gateway

DNS

- Configure DNS for RUSSIA.net
- Create a reverse Zone for the 172.16.0.0/24 network
- Add static records for ALL RU-xx servers

GPO

- Disable "first sign in Animation" on all Windows 10 Clients
- Members of the RU-Users_Experts group must be members of the local admin group on all Windows 10 computers in the domain
- www.russia.net must be the default homepage in IE Explorer and Edge browser
  - Install the Windows_10_Creators_Update_ADMX.msi to make Edge group policies available!
- Disable Recycle Bin on the Desktop for all domain users except users in "RU-Users_Experts" Group and domain administrators
- Disable changing the screen saver for all domain users except users in "RU-Users_Experts" Group and domain administrators
- Disable changing the background picture for all domain users except users in "RU-Users_Experts" Group and domain administrators
- Redirect (Folder redirection) only for all users in the Expert group "my Documents" and the "Desktop" to RU-Files -> d:\shares\redirected
  - share path: \\ru-files.russia.net\redirected\%username%

- Create a fine grained password policy required 7 character non-complex passwords for regular users, 8 characters complex password for members of the RU-Users_Experts group
  - Disable “enforce minimum password age”

Users/Groups

- Create OUs named "Expert", "Competitor", "Manager" and "Visitor"
- Create the following AD groups:
  - RU-Users_Experts
  - RU-Users_Competitors
  - RU-Users_Managers
  - RU-Users_Visitors
  - RU-Project_Budget-R
  - RU-Project_Budget-W
  - RU-Project_Intranet-R
  - RU-Project_Intranet-W
  - RU-Project_Logistics-R
  - RU-Project_Logistics-W
  - RU-DAClients

NOTE: This is a required list of groups and OUs that have to be created in the domain. If you believe that you should create additional groups to perform the tasks you can create them.

- Create the users from the excel sheet RU-Users.xlsx (c:\software) on the competitor machine
  - Fill up all fields in the Active Directory user object and add the users to the corresponding RU-Users_xx groups, RU-Project_xx groups and OUs
- Create for every user a home drive in on RU-Files d:\shares\users.
- Connect the home drive automatically to drive U: -> \\ru-files.russia.net\users$\%username%

NOTE: if you are unable to do import all the users from the Excel file create at least the following users manually

Username/Login	**Password**	**Groups**
Test_expert	P@ssw0rd	RU-Users_Experts; RU-Project_Budget-R
Test_competitor	P@ssw0rd	RU-Users_Competitors; RU-Project_Intranet-W
Test_manager	P@ssw0rd	RU-Users_Managers; RU-Project_Logistics-W
Test_visitor	P@ssw0rd	RU-Users_Visitors

Work Task RU-FILES

This will be the primary file server for the RUSSIA.net domain, but will also provide redundancy for other network services, including DHCP and DNS and AD

INstall/Configure

- Install a Windows Server 2016 (no GUI) from ISO
- When creating the VM, build with 4 drives
  - 1 System drive (c:\)
  - Size 25 GB
  - 1 Raid 5 array with the remaining three drives (d:\)
    - Size 10 GB in **total**
- Rename to RU-FILES
- Configure the network settings as per configuration table/network diagram
- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to RUSSIA.net domain

Shares

- Create shares for departments (Competitors, Experts and Managers)
- on RU-FILES -> d:\shares\departments
  - \\RU-Files\Experts --> d:\shares\departments\Experts
  - \\RU-Files\Competitors --> d:\shares\departments\Competitors
  - \\RU-Files\Managers --> d:\shares\departments\Managers
- Create a share for projects in RU-FILES -> d:\shares\projects
- Create the following folders in d:\shares\projects
  - Budget
  - Intranet
  - Logistics
- Set the permissions for these folders according to the table in the appendix
- Map the project share (\\ru-files.russia.net\projects) to P:\ for all users except the Visitor group
- Users should see only the folders in P:\ where they have permissions to access them (Access-based Enumeration)

Active Directory

- Promote this server as a DC for RUSSIA.net (but not a GC)

DFS

- Create a Namespace with the name “dfs”
- Add RU-DC as the second server for this Namespace
- Create DFS links for the department shares (Experts, Competitors, Managers)
- Create a DFS Replication to implement a backup of the department shares on RU-DC. The shares should be replicated/backed up like this:
  - RU-Files: D:\shares\departments\Experts → RU-DC: C:\backup\Experts
  - RU-Files: D:\shares\departments\Competitors → RU-DC: C:\backup\Competitors
  - RU-Files: D:\shares\departments\Managers → RU-DC: C:\backup\Managers
- Map the department shares depending on the corresponding group (RU-Users_Experts, RU-Users_Competitors, RU-Users_Managers) to drive G: using the DFS Namespace

DHCP

- Install and configure DHCP
- Mode: Load balancer
- Partner Server: RU-DC
- State Switchover time: 10 minutes

DNS

- Host RUSSIA.net forward and reverse lookup zones

Quota/Screening

- Set the quota to every home drives to 5GB
- Prevent storing .cmd and .exe files on the home drives. All other file extensions are allowed!

Customized error messages

- Make sure that unauthorized users get the following error message, when they want to access one of the three department shares (Experts, Competitors and Managers) they are not allowed to!
    - Expert share:
        - Error message: “Access only for EXPERTS allowed”
    - Competitor share:
        - Error message: “Access only for COMPETITORS allowed”
    - Manager share:
        - Error message: “Access only for MANAGERS allowed”

IIS

- Create a website for the managers (use the provided html file as the default page from C:\software on the competitor computer)
- This website should be accessible via managers.russia.net
- Only users in the in RU-Users_Managers group should have access to the website using "user certificate based authentication"

Work Task RU-ROOTCA

This will be the ROOT Certificate authority for the PKI infrastructure.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- DO NOT join this server to any domain

Install AD CS services

- standalone Root CA – Use default key length, hash, etc. if not specified
- Name: RUSSIA Root CA
- Lifetime: 10 years
- CRL location: http://RU-SUBCA.russia.net/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl
- AIA location: http://RU-SUBCA.russia.net/certenroll/<serverdnsname>_<caname><certificatename>.crt
- Create certificate revocation list, and necessary root certificates for RU-SUBCA, and export them to RU-SUBCA, via share or any other method
- Approve subordinate Certificate request from RU-SUBCA
- Take the server offline when not in use (**disable the network interface only**)

Work Task RU-SUBCA

This will be the online subordinate CA in the PKI infrastructure.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join the machine to the RUSSIA.net domain

Install AD CS and Web Enrolment services

- Install Enterprise Sub CA
- Name: RUSSIA Sub CA
- Import and publish CRL for Root CA
- Lifetime: 5 years
- Configure a template for all clients called "_Skills39_RUClients"
  - Set the "subject name format" to Common Name
  - Auto enroll this template to all RUSSIA.net Windows 10 Clients
- Configure a template for a group of users called "_Skills39_SpecialUsers"
  - Set the "subject name format" to Common Name
  - Auto enroll this template only to the RU-Users_Managers group
- Create the necessary certificates for the two websites on AE-IIS

Work Task RU-CLIENT

This is a Windows 10 client in the RUSSIA.net domain and can be used for regular user or administration of the RUSSIA.net servers and test DirectAccess from the "Internet"

Note: Set the power settings to "never sleep" for all Windows 10 clients

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join the client to the RUSSIA.net domain
- Install the RSAT tools for server management
- Use this client for testing the DirectAccess connection
- Use this client for testing the GPO settings

NOTE: for testing the Direct Access connection you have to switch this client to the INTERNET Network

Part 2 – UAE.net

In Part 2 you will responsible for making the existing infrastructure available for remote clients, connectivity to the new domain and maintaining the website information for both

NOTE: Refer to the diagram on the last page for quick specification reference, as well as the configuration table.
Please use the default configuration if you are not given the details
Local, domain and existing passwords will be "P@ssw0rd"

Work Task AE-DC

This is the existing domain controller for the old domain and hosts all the user and group information

Install/Configure

- already preinstalled (domain UAE.net, Users, DNS, DHCP)

Copy Users to Russia.net

- All user with "Expert" in the "Job Title:" should have duplicate accounts created for them in the RUSSIA.net domain (we are not using GPMT – so it is not a migration just a re-creation of the user accounts)
    - Copied Users should be placed to OU "Migration" in RUSSIA.net
    - Set the password to "WorldSkills2017mig"
    - Copy the necessary home folders from AE-DC to RU-FILES d:\shares\migrated
    - Set the necessary permissions on these copied folders/shares (only the user itself and domain administrators should have access to these homefolders)
    - Map the home folder to drive S:\ automatically (\\RU-Files\migrated$\%username%)
    - Disable the copied users in UAE.net and move them to a new OU called MIGRATED on AE-DC

AD

- Create the following three users in OU “Users”. They are necessary for the following work tasks.
    - RDS_user1
    - RDS_user2

Shares

- Create a share for the BitLocker recovery keys.
    - \\AE-DC\bitlocker --> C:\shares\bitlocker

DNS

- DNS records should point to the correct IP addresses for both www.UAE.net and www.RUSSIA.net
- DNS records should point to the correct IP address to the RemoteApp website.

Work Task AE-IIS

This server hosts your current UAE.net website and need to have the content for the RUSSIA.net added to your network to provide access to the new RUSSIA.net domain

IIS

- Host www.UAE.net website
    - Move the default website from wwwroot to c:\inetpub\uae
- Host www.RUSSIA.net website (provided) in c:\inetpub\russia
- Both websites should be available by hostname
- Both of these sites should use https using certificate approved in RUSSIA.net

Work Task AE-RDS

This server is used for Published Applications in the UAE.net domain.

Install/Configure

- Install Windows Server 2016 from ISO
- Rename to AE-RDS
- Configure the network settings as per configuration table/network diagram
- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to UAE.net domain

Remote Desktop Services

- Install Remote Desktop Services
    - Do not install RD Licensing component.
- Configure web-access for terminal services.
- The RDS login page should be accessible by entering the URL https://rds.uae.net
- On the RU-SUBCA server, generate and use the corresponding SSL certificate for terminal services. Apply this certificate for all components of the terminal services. When connecting to the website https://rds.uae.net from any computer in the UAE.NET domain, the certificate must be trusted and valid (no certificate warning should be shown).
- Make sure, only users RDS_user1 and RDS_user2 are able to login via RDP.
- Publish Wordpad on the web-portal of RemoteApp for the domain user “RDS_user1”
- Publish Notepad on the web-portal of RemoteApp for the domain user “RDS_user2”

Work Task AE-CLIENT

Note: Set the power settings to "never sleep" for all Windows 10 clients

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join the client to the UAE.net domain
- Use this client for all tests in the UAE.net domain

BitLocker

- Encrypt the system drive using BitLocker
- Use the password “P@ssw0rd”
- Save the recovery key in the share \\AE-DC\bitlocker\ on AE-DC with the filename “AE-Client_recovery-key.txt”

Work Task AE-REMOTE

Note: Set the power settings to "never sleep" for all Windows 10 clients

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- DO NOT join this client to any domain

VPN

- Configure the VPN client settings for all users on this computer
    - Connect the VPN using the public IP of AE-EDGE
    - Use IKEv2 protocol with machine certificate authentication

Use this client for testing the "external" access to the websites

- www.russia.net and www.uae.net

Part 3 – INTERNET/VPN/REMOTE ACCESS

In Part 3 you have to setup remote access to the RUSSIA.net domain for the clients, Site-to-Site VPN between the two networks/domains and a client VPN solution for the UAE.net domain.

NOTE: Refer to the diagram on the last page for quick specification reference, as well as the configuration table.
Please use the default configuration if you are not given the details

Work Task INET

Note: This server has already been preconfigured with all the necessary settings for "simulating the internet in a test lab" and also DHCP is already setup.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic

DNS/IIS

- Create the appropriate resource records (DNS) for external access to the Direct Access server in the RUSSIA.net domain and also for www.UAE.net and www.RUSSIA.net websites access.

Work Task AE-EDGE

This is the VPN server that will allow access for external clients to the internal network. It will also create a VPN tunnel to the RUSSIA.net domain.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to UAE.net domain
- Install RRAS service
- Install server authentication certificate from RU-SUBCA

NAT configuration

- Port mapping for external access to AE-IIS websites
    - Both RUSSIA.net and UAE.net web content (verify from AE-REMOTE)

VPN

- Configure VPN for client access.
- Use the IKEv2 protocol and make sure authentication is done by client certificate
- Use the IP range 172.19.0.50 – 172.19.0.79
- The VPN clients should have access to all internal networks (UAE.net and RUSSIA.net)

Site-to-Site VPN

- Configure Site-to-Site VPN to RU-EDGE server
- Use machine certificate for the authentication
- Set the connection type to “persistent connection”
- All traffic bound for RUSSIA.net will be placed in the VPN tunnel

Work Task RU-EDGE

This is the VPN and DirectAccess server that will allow access for external clients to the internal network. It will also create a VPN tunnel to the old UAE.net domain.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to RUSSIA.net domain
- Install server authentication certificate from RU-SUBCA

Configure Direct Access

- Add RU-Client to the AD group "RU-DAClients"
- Only members of "RU-DAClients" group can use remote connection
- Use RU-FILES server as the only NCA
- Generate SSL certificate on the PKI and use it for client connections (no self-signed certs are allowed)
- DirectAccess connection name "my W@rkplace"
- Use connect.russia.net for the access from the internet
- The DA clients must get full access to the resources of RUSSIA.net network and UAE.net

Site-to-Site VPN

- Configure Site-to-Site VPN to the AE-EDGE server
- Use machine certificate for the authentication
- Set the connection type to “persistent connection”
- All traffic bound for UAE.net will be placed in the VPN tunnel

Configuration Table

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
AE-DC	Windows Server 2016 GUI	UAE.net	172.19.0.1/24	Yes - configured
AE-CLIENT	Windows 10	UAE.net	DHCP	Yes - configured
AE-IIS	Windows Server 2016 no GUI	UAE.net	172.19.0.3/24	Yes - configured
AE-RDS	Windows Server 2016 GUI	UAE.net	172.19.0.2	NO
AE-EDGE	Windows Server 2016 GUI	UAE.net	172.19.0.250/24 200.100.50.101/24	Yes - configured
RU-DC	Windows Server 2016 GUI	Russia.net	172.16.0.1/24	Yes - configured
RU-FILES	Windows Server 2016 no GUI	Russia.net	172.16.0.2/24	NO
RU-ROOTCA	Windows Server 2016 GUI	None	172.16.0.3/24	Yes - configured
RU-SUBCA	Windows Server 2016 GUI	Russia.net	172.16.0.4/24	Yes - configured
RU-EDGE	Windows Server 2016 no GUI	Russia.net	172.16.0.250/24 200.100.50.100/24	Yes - configured
RU-CLIENT	Windows 10	Russia.net	DHCP	Yes - configured
AE-REMOTE	Windows 10	None	DHCP	Yes - configured
INET	Windows Server 2016 GUI	None	200.100.50.200/24	Yes - configured

Machines indicated as being preinstalled with "**Yes – configured**" will have the operating system installed and Hostname and network settings configured.

Shares/Permission Table

Sharename	Location	Read access group	Read/Write access group
Budget	RU-Files -> D:\shares\projects	RU-Budget-R	RU-Budget-W
Intranet	RU-Files -> D:\shares\projects	RU-Intranet-R	RU-Intranet-W
Logistics	RU-Files -> D:\shares\projects	RU-Logistics-R	RU-Logistics-W

4. INSTRUCTIONS TO THE COMPETITOR

- 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 you starting work.
- Be aware different tasks attract a percentage of the overall mark. Plan your time carefully.
- If your virtual machines spontaneously turned off, run slmgr /rearm command with the administrator credentials

5. EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

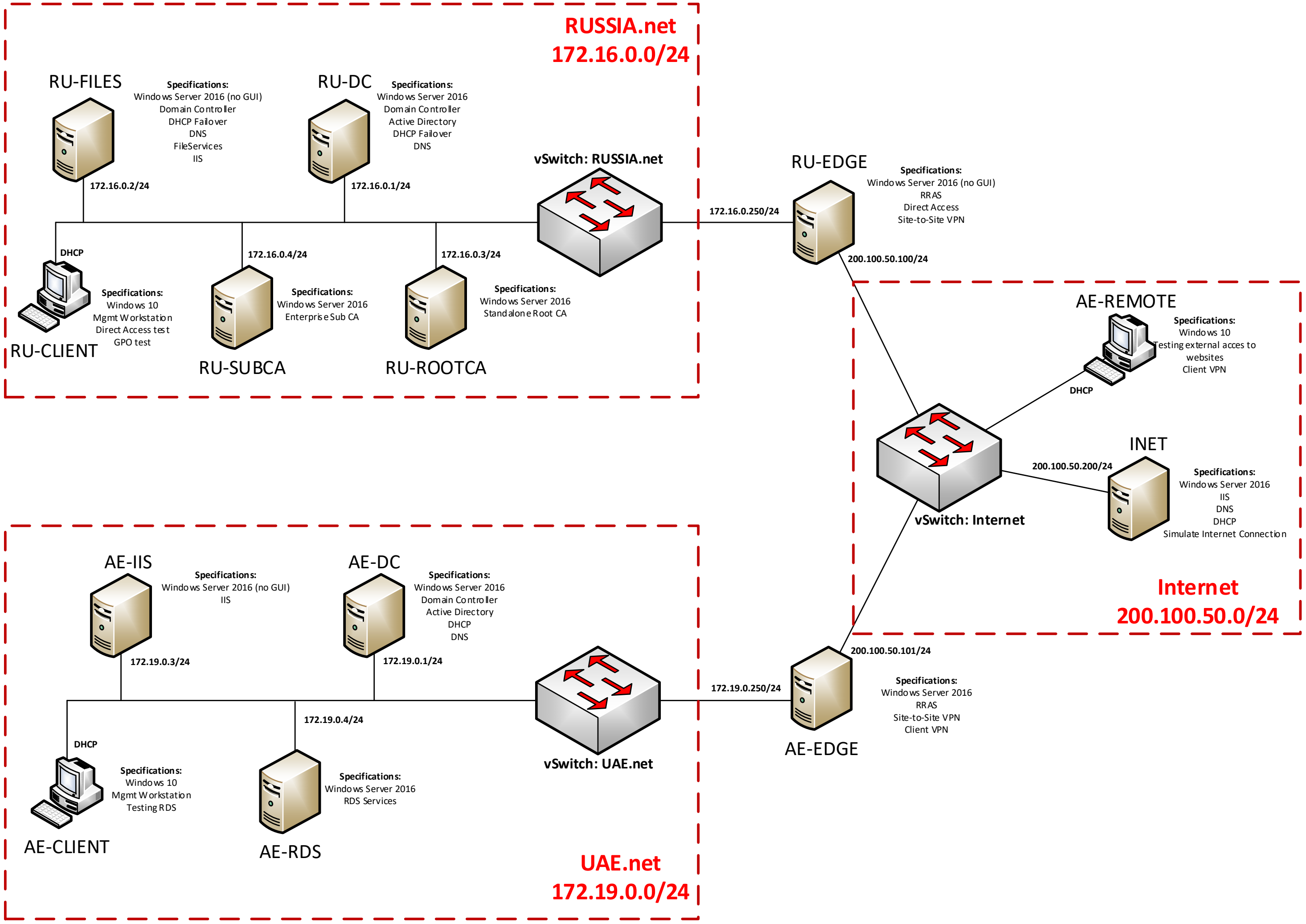
Standard/Administration-PC

Intel i5 processor
16GB RAM
500GB SSD-Drive
1x24 inch LED-Monitors
US Keyboard
Mouse

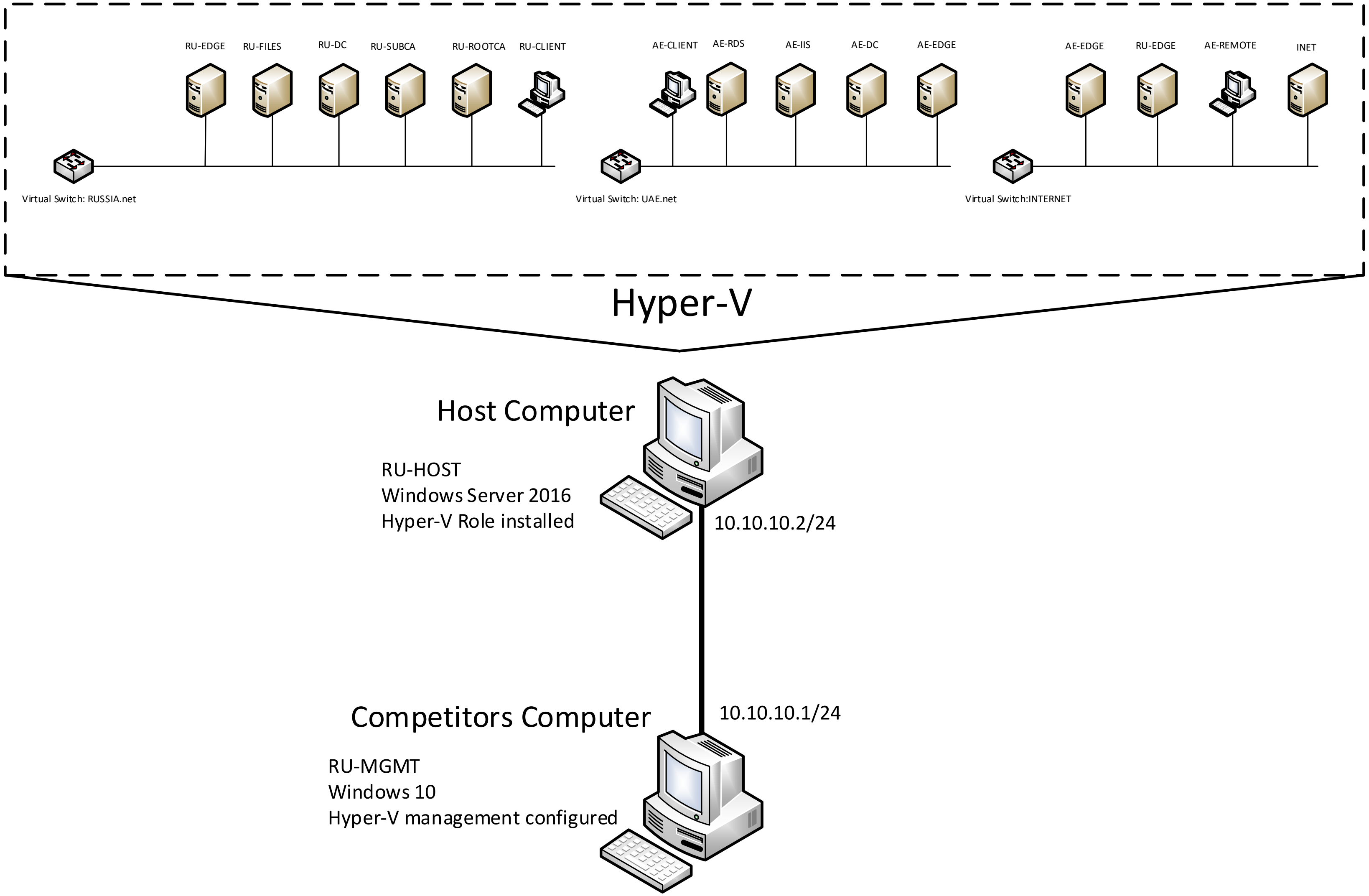
Highspec/Host-PC

Intel i7 processor
64GB RAM
500GB SSD-Drive
1x24 inch LED-Monitor
US Keyboard
Mouse

6. NETWORK DIAGRAM



7. PHYSICAL NETWORK DIAGRAM


RU-EDGE
RU-FILES
RU-DC
RU-SUBCA
RU-ROOTCA
RU-CLIENT
Virtual Switch: RUSSIA.net
AE-CLIENT
AE-RDS
AE-IIS
AE-DC
AE-EDGE
Virtual Switch: UAE.net
AE-EDGE
RU-EDGE
AE-REMOTE
INET
Virtual Switch:INTERNET
Hyper-V
Host Computer
RU-HOST
Windows Server 2016
Hyper-V Role installed
10.10.10.2/24
10.10.10.1/24
Competitors Computer
RU-MGMT
Windows 10
Hyper-V management configured