Design document

Case Study

Robert Ašvicas

Dmitry Lvov

Tutor:

Mikaeil Shaghelani

Date:

2020-04-21

**Contents**

[Introduction 3](#_Toc38376935)

[Roles and actors 3](#_Toc38376936)

[Infrastructure of our environment 4](#_Toc38376937)

[System setup 5](#_Toc38376938)

[Virtual Machines 5](#_Toc38376939)

[Windows Active Directory 5](#_Toc38376940)

[Windows Client Machine 5](#_Toc38376941)

[Linux Server 5](#_Toc38376942)

[Firewall 5](#_Toc38376943)

[Group policies 6](#_Toc38376944)

[VPN 7](#_Toc38376945)

[Folder Redirection 7](#_Toc38376946)

[MoSCoW 8](#_Toc38376947)

# Introduction

The company “Make IT Work4U” wants to mimic IT infrastructure of a customer. Our job is to setup the whole environment for that. That includes infrastructure and application/dashboard to monitor server conditions.

# Minimal requirements

* Virtual Servers to simulate environment
  + Windows AD
  + Windows for client
  + Linux
  + Firewall
* Different users and group policies in simulated environment
* Application/dashboard
  + Real-time statistics
  + Database
  + Logs

# Roles and actors

**Clients** supposedly will connect to Windows Client using one of few created accounts. They will be able to share files, access internet, but they will not have access to configuring server.

**Administrators** will be able to connect to all machines and configure it how it is needed at that moment. They have full access to all machines.

# MoSCoW

Our prioritization of tasks:

**Must have:**

* Windows server with Hyper-V
  + Configured Networking
    - DNS
    - DHCP
    - Firewall
    - Proxy
    - VPN
  + Configured AD usage
    - Users
    - Policies
    - Folder Redirection
* Application for server:
  + Server health stats
  + Virtual machine stats
  + Log management (creating, tracking, sorting)
  + Database tracking
* Linux server
* Backup policies

**Should have:**

* Windows server
  + More users
  + Advanced User Policies
* Application
  + Graphical diagrams of real time statistics
  + In-depth information about the server users such as uptime and application they are using at that moment

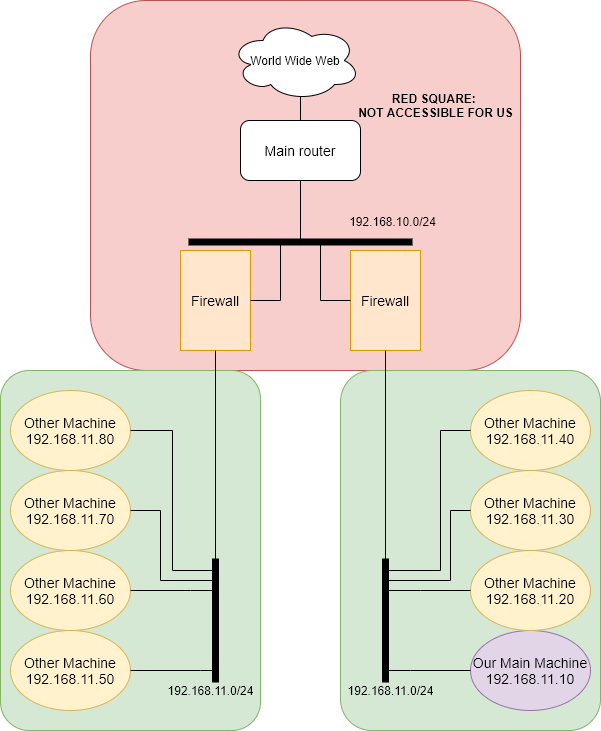
**Could have:**

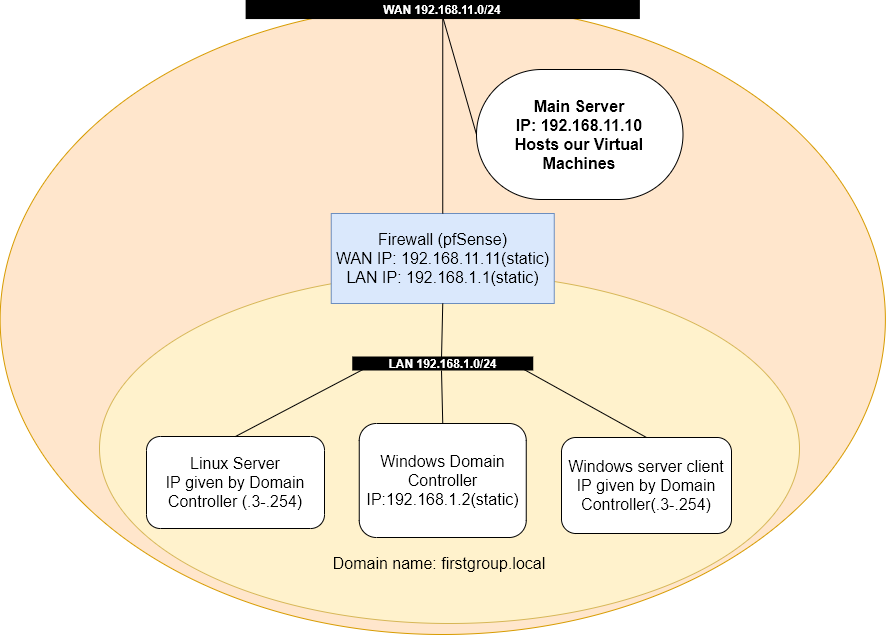
* Windows server
  + Backup on external device
  + AdBlock
  + Proxy + Anti-Virus
  + Intrusion Detection System
* Application
  + Graphs with real-time + past statistics for main system components
  + Visual implementations for easier observation of main system functionality
  + Different color themes

**Won’t have:**

pass

# Infrastructure of our environment





# System setup

One server is hosting 8 Virtual Machines, one of them we will consider as our Main Machine, since we can connect only to it. Our Main Machine is hosting 4 Virtual Machines using Hyper-V, native hypervisor included in Windows Server. On the Hyper-V we have installed Windows with Active Directory (Domain Controller), Windows for clients to connect to, Linux Server (Lubuntu) and Firewall (pfSense). More specific details about each one will follow.

# Virtual Machines

All those VMs are in the same domain name, which is called firstgroup.local. All of them have Dynamic Memory and they are 2nd generations VM, so disk space is also dynamic. They are in the network

## Windows Active Directory

Windows Active Directory is responsible for giving out IP addresses (it has DHCP Server installed on it), DNS server, and hosting domain called firstgroup.local. Also, through AD we are managing group policies. This machine has IP 192.168.1.2, netmask 255.255.255.0 and gateway 192.168.1.1, all this is statically configured. In Hyper-V this VM is called “Win2019\_AD”.

## Windows Client Machine

Windows Client Machine is machine made for users to connect to. It shares folders: Documents and Desktop. It is designed mainly for users to connect to it. This machine will be given IP by DC (Domain Controller) (Scope: 192.168.1.3-.254) (most commonly it’s given 192.168.1.3 IP). In Hyper-V this VM is called “Win2019\_not\_AD”.

## Linux Server

Linux server has Lubuntu running on it. It server experimental purposes. In Hyper-V it’s called “Linux”.

## Firewall

pfSense serves as a router and a firewall. It connects 2 networks – WAN and LAN. Without firewall firstgroup.local domain won’t have any internet connection. WAN IP: 192.168.11.11/24 – static configuration, gateway 192.168.11.1. LAN IP: 192.168.1.1/24 – static configuration. Firewall forwards DNS queries firstly to DC, then it checks itself, and only then in forwards it outside.

Firewall has Proxy server enabled on it. In our case proxy is working as a caching server.

In Hyper-V this VM is called “Firewall”.

# Group policies

There is a main policy called GTA which applies the same background pictures for user-group SanAndreas which has 2 users, CJ and Big Smoke. Apart from that we’ve implemented a folder redirection option which communication-wise allows users to share Documents folder.

Groups:

* Administrators
  + Users
    - Admin
    - Administrator
    - Test
  + Policies
    - Full system control
    - Folder Redirection
* SanAndreas
  + Users
    - CJ
    - Big Smoke
  + Policies
    - GTA (Unified background picture)
    - Folder Redirection

# VPN

Server:

As a VPN server we’ve chosen OpenVPN as it satisfies all our necessities and it is easy to configure and use. The server was configured with default settings which means that the only parameter that we’ve had to change manually was “Tunnel network” 10.0.10.0/24 and DNS domain (firstgroup.local) with servers which are 192.168.1.2 and 127.0.0.1. The server uses basic encryption with self-signed certificate for users who want to connect to it.

Client:

For each user that will use VPN network there will be a separate private account with login and password credentials which they are going to use through Viscosity client to connect to the network. Port redirection allows users to enter the public IP and certain port which will be assigned to them to connect to the network.

# Folder Redirection

Communication-wise all users in the system will use folder redirection function in regards of Documents and Desktop folder. As users remain in the same network, they have possibilities of using the same Documents and Desktop folders which originate from the Windows VM with AD. This option will allow users to exchange information on a higher pace and with better efficiency.

# Backup Policy

Backups are setup on our Main Machine, it can be accessed via Server Manager -> Tools -> Windows Server Backups. It is backup-ing “Firewall” VM every day at 03:00AM. The backup is stored in shared network folder called “Backup” in Drive C, which is not secure, but right now, it’s the only way to do it (For other ways we have insufficient disk space).

# Application

Application/dashboard is made in Python programming language, which is also installed on our Server. Python version is 3.8.2. For developing GUI we have used Tkinter, for taking