RAM = up 2GB SystemHDD = up 20GB

Install Windows -> Activate Windows -> Account Password: xxxx.xxxx (има изискване за сложност на паролата)

Router before Local Network:

Gateway: 192.168.1.1

Server IP: 192.168.1.52

пренасочени Port WAN -> LAN 192.168.1.200

пренасочени 80 WAN -> 80 192.168.1.52 TCP/UDP

пренасочени xxxxx1 WAN -> 21 192.168.1.51 TCP

пренасочени xxxxx5 WAN -> 3389 192.168.1.51 TCP/UDP Remote Desktop Port

пренасочени 8868 WAN -> 8868 192.168.1.200 TCP/UDP

пренасочени 443 WAN-> 443 192.168.1.200 TCP/UDP

Control Panel -> System and Security -> Administrative Tools

1. Първоначална настройка

Administrative Tools -> Services ->

Windows Updates Stop -> Disabled

Windows Error Reporting Service Stop -> Disabled

Windows Defender Stop -> Disabled*

Windows Audio Manual -> Start

Function Discovery Resource Publication Manual -> Start

SSDP Discovery -> Automatic -> Start

UPnP Device Host -> Automatic -> Start

DNS Client -> Automatic -> Start

Administrative Tools -> Local Security Policy ->

Security Settings -> Local Policies -> Security Options => Interactive logon: Do not require CTRL+ALT+DEL = Enabled => Apply

2. Настройват се мрежовите карти

Control Panel -> Network and Internet -> Network and Sharing Center ->

-> Change adapter settings

Input LAN: auto

Output LAN:

-right click-> Properties on network card -> Select – Internet Protocol Version 4 (TCP/IPv4) -> Click Properties ->

LAN: 192.168.0.1 255.255.255.0

No -> (Advanced -> WINS tab -> enable NetBIOS over TCP/IP)

-> Change advanced sharing settings –select-> Public ->

(*) Turn on network discovery

(*) Turn on file and printing sharing

(*) Turn off Public folder sharing

(*) Turn on password protected sharing -> Save Changes

(Out v6 LAN 0:0:0:FFFF:192:168:0:1 /64)

3. Променя се името на сървъра

Control Panel -> System and Security -> System -> Remote settings ->

Computer Name -> Change… ->

Computer Name: SERVER-HOME

Workgroup: WORKGROUP -> OK -> Restart

4. Разрешава се дистанционен достъп

(през Internet се използва порт 3389, до 2 юзера се допускат без инсталиран разширения Remote Desktop)

Control Panel -> System and Security -> System -> Remote settings -> Remote ->

(*) Allow connections from computers running any version of Remote Desktop -> Select Users... -> Add… --> Advanced --> Find Now -> Administrator(XXX) -> OK -> OK -> OK

Control Panel -> System and Security -> Windows Firewall -> Allow a Program through Windows Firewall

-Check-> Remote Desktop

-Check-> Routing and Remote Access

-Check-> File and Printer Sharing

-Check-> Network Discovery

Ако е лаптоп се изключват в захранващите опции Sleep:

Control Panel -> System and Security -> Power Options

(*) High performance

Change Plan Settings -> Change advanced power settings

5. Включват се DHCP и други функции

Control Panel --> Administrative Tools -> Server Manager -> Roles -> Add Roles

[v] Network Policy and Access Services -> Next

[v] Routing and Remote Access Services -> Next -> Install

[v] DHCP Server -> Next -> Next -> Next

Parent domain: vega-bg.com*

[v] Web Server (IIS) -> Next

[v] Application Development

[v] "All Function"

[v] Security

[v] Basic Authentication

[v] Regvet Filter

[v] FTP Server

[v] All

[v] IIS Hostable Web Core

Настройват се поотделно функциите (виж по-нататък индивидуалните настройки)

-> Install (изчаква се по-дълго време) -> Close

Administrative Tools -> Services ->

Routing and Remote Access: Automatic -> Apply -> Start

Microsoft FTP Service: Automatic

DHCP Server: Automatic -> Start

Ако не може да се стартира "Access Denied Error 5" направете следното:

Windows Button + RUN -> regedit -> OK

HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> services -> DHCPServer - right button-> Permissions... -> DHCPServer -> [v] Full Control -> OK

6. Настройва се DHCP сървъра

Control Panel -> Administrative Tools -> DHCP

IPv4 -right button-> New Scope... -> Next

Name: Local Network

Description: /clear/ -> Next

Start IP address: 192.168.0.2

End IP address: 192.168.0.254

Length: 24

Subnet mask: 255.255.255.0 -> Next

Add Exclusions and Delay: 192.168.0.80 to 192.168.0.99 -> Add -> Next

Lease Duration 10 Days -> Next

Configure DHCP Options

(*) Yes, I want to configure these option now -> Next

Router (Default Gateway) 192.168.0.1 -> Add -> Next

Parent domain: /clear/

Server name: www.lz4gv.com /това ще се изписва на потребителите/

IP adderss: 212.39.90.42 -> Add

IP adderss: 212.39.90.43 -> Add -> Next

За Виваком: 212.39.90.42 212.39.90.43

За М-Тел: 213.226.7.34 213.226.7.35

WINS Servers: /clear/ -> Next

(*) Yes, I want to activate thise scope now -> Next -> Finish

ако използваме IP v6

IPv6 -right button-> New Scope... -> Next

Name: home-v6

Description: /clear/ -> Next

Prefix ::FFFF:192:168:0:0 /64

Preference: 0 -> Next

Start IPv6 Address ::FFFF:192:168:0:2

End IPv6 Address ::FFFF:192:168:0:FFFF -> Add -> Next

Preferred Temporary Adress(IANA): 8Days

Valid Life Tima: 12Days -> Next -> Finish

7. Избираме адаптери за входящ и изходящ трафик

включваме Internet

Administrative Tools -> Routing and Remote Access

SERVER-HOME(local) -right button-> Configure and Enable Routing and Remote Access

(*) Network Address Tranlation (NAT) -> Next -> Finish

Пренасочване на портове

IPv4 -> NAT -> (Internet Input Card) -right button-> Properties

Services and Ports -> Add... -> IP camera

[*] On this interface

[*] TCP

Incoming Port: 40002

Private address: 192.168.0.126

Outgoing port: 81 -> OK -> Apply

Пренасочих Порт 445 към порт 80 на устройство в локалната мрежа – спряха атакита през SMB

8. Настройка на дистанционен достъп за много клиенти

Изключваме сървъра и интернета -> променяме годината в BIOS на 2030 -> включваме

Control Panel --> Administrative Tools -> Server Manager -> Roles -> Add Role

[v] Remote Desktop Services -> Next -> Next

[v] Remote Desktop Session Host -> Next

(*) Do not require Network Level Authentication -> Next

(*) Configure later -> Next

[v] Audio and Video Playback

[v] Audio Recordin redirection

[v] Desktop composion (.....)

-> Install -> Restart –изчаква се повече да зареди отново акаунта -> Close

Изключваме сървъра -> възстановяваме годината в BIOS на текущата -> включваме

---

9. Настройва се Web сървъра

Administrative Tools --> Internet Information Services (IIS) Manager

XXX(local computer) -> Sites -right button-> Add Web Site...

Site name: test.com

Phisical path: C:\.....

Type: http

IP: 46.10.100.81 (външно IP на мрежовата карта свързана с интернет)

TCP Port: 80

Host name: www.test.com

IIS -> Default Document -> Add: index.html (Move Up)

Directory Browsing -> Enabled (от дясната страна)

Start -> Windows Explorer

Select Folder Web Seties -Right Click-> Properties -> Security

Edit... -> Add... -> Advansed... -> Find Now -> IIS_IUSRS -> OK -> OK -> OK

10. Настройва се FTP сървъра

Administrative Tools --> Internet Information Services (IIS) Manager

XXX(local computer) -Right Buton-> Add FTP Site…

FTP site name: NAS

Physical path: D:\..... (Browse...)

IP: 46.10.100.xx (IP на входната мрежова карта)

TCP Port: 21 (или друг порт)

[v] Start FTP site automatically

[*] No SSL -> Next

[v] Basic OK

Allow access to: All users [v] Read [v] Write

(ftp_files) -> FTP Authorization Rules -> Add Allow Rule…

[*] All Users

[v] Read [v]Write -> OK

11. Добавяне на юзери

11.1 Забрана на изискването за сложност на паролите.

Administrative Tools -> Local Security Policy -> Account Policies -> Password Policy

Password must meet complexity requirements: (*) Disabled

Maximum password age: 0 days

-Start-> Command Prompt –напиши-> GPUpdate /force

11.2 Добавяне на акаунти

Administrative Tools -> Computer Management -> Local User and Groups -> Users

-right button-> New User

User name:

[*] Standard user

-select User-> Create Password

акаунта трябва да е заключен с парола!

11.3 Създаване на група от потребители

Contol Panel -> Administrative Tools -> Computer Management -> Local User and Groups -> Groups

-right button-> New Group...

Group name: Home

Members: -> Add... -> Advanced... -> Find Now

добавяме Юзери -> OK -> OK -> Create

11.4 Разрешава се дистанционен достъп на клиентите.

Contol Panel -> Administrative Tools -> Computer Management -> Local User and Groups -> Groups

Remote Desktop Users

-right button-> Add to Group... -> Add... -> Advanced... -> Find Now

добавяме Юзери -> OK -> OK

---

12. Настройка на дисковете

Security -> SYSTEM – Full Control

Administrator**s** - Full Control

Users - ……

Everyone – Removed

Sharing -> Advanced Sharing…

[v] Share these folder

Share name: NAS

Permissions: **Remove “Everyone”**

Add -> Users or Groups…….. -> Full control

Ако загубим достъп до файловете:

Owner -> Current owner: Administrators

[v] Replace owner on …..

Permission -> Change Permission –select all-> Remove -> Apply

-> Add -> -> Everyone -> Full Control Allow

[v] Replace all child objects -> Apply

Също може да ги преместим на диск с пълен контрол и после да ги върнем на чисто място

13. Настройка на антивирусната програма Symantec Endpoint Protection

Change settings -> Network Theat Protection -> Firewall

Build-in Rules

All Disable

Unmatched IP Traffic Settings

[*] Enable denial…

[*] Enable port scan…

[*] Allow IP traffic – позволява преноса на интернет към вътрешната мрежа

Active Response Settings

[ ] Number of seconds to automatically... 600

Stealth Settings

[ ] Enable TCP resequencing - позволява да се отваря Web страниците от вътрешната мрежа, спира прекъсването на файл трасфера.

[ ] Enable OS fingerprint masquerading -

[ ] Enable stealth Web browsing

---

14. Активиране на Backup

Server Manager -> Features -> Add Features

Windows Server Backup Features -> Next -> Install

Control Panel -> Administrative Tools -> Windows Server Backup

Backup Once…..

[*] Differen options

[*] Custom

Add Intems……..

Advanced Settings

VSS Settings

[*] Vss full Backup -> OK

[*] local Drives……..

15. Настройки при пренасочване на принтери.

C:\Windows\System32\Spool –right button-> Properties -> Security -> Edit… ->
Authenticated Users -> [v] Full Control

Win+R -> gpedit.msc
Computer configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Printer Redirection

Use Remote Desktop Easy Printer printer driver first -right button-> Disabled

14.1. Добавяне на драйвери за други принтери.

Devices and Printers -> Add a printer -> Add a local printer -LPT1-> Next -> Windows Update ....time...

---

16. Премахване на създаването на Thumbs.db файлове

Win+R gpedit.msc
User Configuration -> Administrative Templates -> Windows Components -> Windows Explorer -> Turns off the caching of thumbnails in hidden thumbs.db files: Enabled
Log off -> Log on

---

17. Допълнителни настройки

При смяна на доставчика на Internet

DHCP

Server-XXX -> IPv4 -> Scope [192.168.0.0] -> Scope Options -> 006 DNS Servers –right button-> Properties -> IP Address -> Add DNS от доставчика

Routing and Remote Access не е задължително

Disable Routing and ….

Configure and Enable Routing

активиране на Wi-Fi адаптера

Administrative Tools -> Server Manager -> Features -> Add Features

[v] Wireless LAN Service -> Install

XX. Ако от друг компютър отваряме програма намираща се на сървъра да не изважда предупреждаващ прозорец.

Disable Windows 7's "Open File - Security Warning"

Widows Button + R -> gpedit.msc

User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager

-> Inclusion list for low file types -> (*) Enable -> .exe;.dba;.xls

---

Настойка на SQL Server:

SQL Server (MSSQLSERVER) - Automatic -> Started/Manual

Portable Device Enumerator Service - Maual/Stop -> Disable

Start -> Microsoft SQL Server 2008 R2 -> Cofiguration tools -> SQL Server Configuration Manager

SQL Server Services -> SQL Server (MSSQLSERVER) -> Properties

Built-in account: Local Service

Client Protocols: TCP/IP – Disabled For All

Widows Firewall -> Advanced settings -> Inbound Rulles:

SQL Server: Disable (*) Block the connection

Core Networking: --//--

Задайте правило за блокиране на профила

Като настроите компютъра си да заключва акаунт за определен период от време след няколко неправилни предположения, вие ще попречите на хакерите да използват автоматизирани средства за познаване на пароли, за да получат достъп до вашата система (това е известно като атака "груба сила"), , За да зададете правила за блокиране на профили:

Go to Start --> Programs --> Administrative Tools --> Local Security Policy

Under Account Policies --> Account Lockout Policies

Account lockout threshold: 3 Тази настройка за сигурност определя броя неуспешни опити за влизане, които причиняват заключване на потребителски акаунт. Забраненият профил не може да бъде използван, докато не бъде възстановен от администратор или до изтичане на срока на блокиране за профила. Можете да зададете стойност между 0 и 999 неуспешни опити за влизане. Ако зададете стойността на 0, профилът никога няма да бъде заключен.

Reset account lockout counter after: 5 Тази настройка за сигурност определя броя на минутите, които трябва да изминат след неуспешен опит за влизане, преди неуспехът на брояча за опит за влизане да бъде нулиран до 0 лоши опити за влизане. Предлаганият диапазон е от 1 минута до 99,999 минути.

Account lockout duration: 5 Тази настройка за сигурност определя броя минути, през който заключен акаунт остава заключен, преди автоматично да се отключи. Предлаганият диапазон е от 0 минути до 99,999 минути. Ако зададете продължителността на блокирането на профила на 0, профилът ще бъде заключен, докато администраторът изрично не го отключи. Ако е определен праг за блокиране на профила, продължителността на блокирането на профила трябва да е по-голяма или равна на времето за нулиране.

Променете порта за слушане за отдалечен работен плот

Промяната на порта за слушане ще помогне да се "скрие" отдалечен работен плот от хакери, които сканират мрежата, за да слушат компютрите на порт по подразбиране за отдалечен работен плот (TCP 3389).

Windows Button + RUN -> regedit -> OK

HKEY HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp -> PortNumber: Променете порта за слушане от 3389 в нещо друго

Не забравяйте да актуализирате всички правила на защитната стена с новия порт.

Windows Firewall -> Advanced Settings -> Inbound Rules:

Remote Desktop (TCP-In)

Remote Desktop – RemoteFX (TCP-In)

Windows Firewall -> Outbound Rules

Distributed Transaction coordinator (TCP-Out) -> Allow