CP 2 Document

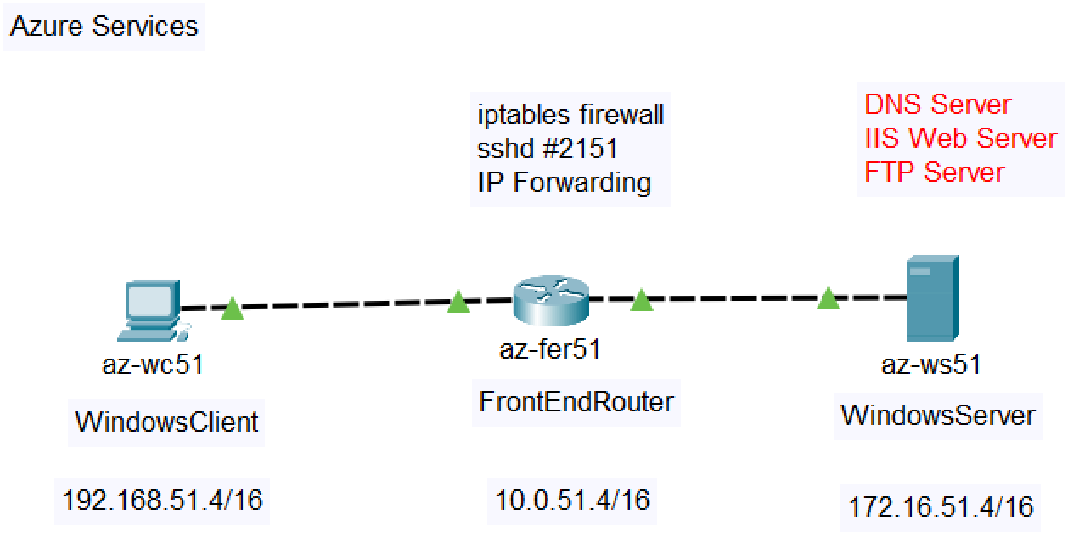
12 FEB 2021
NDD430B

Student: FATJON DAUTI
Instructor: SCOTT APTED

Table of Contents

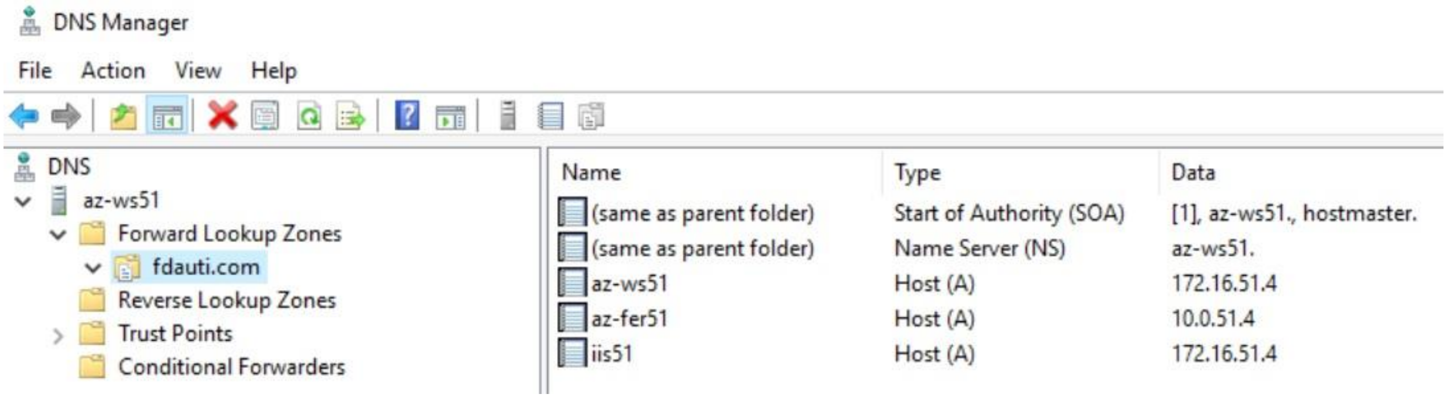
Create a Network Diagram that displays the topology of your Azure network and includes:

- **IP addressing information for all interfaces**
- **A list of services being hosted by each device**



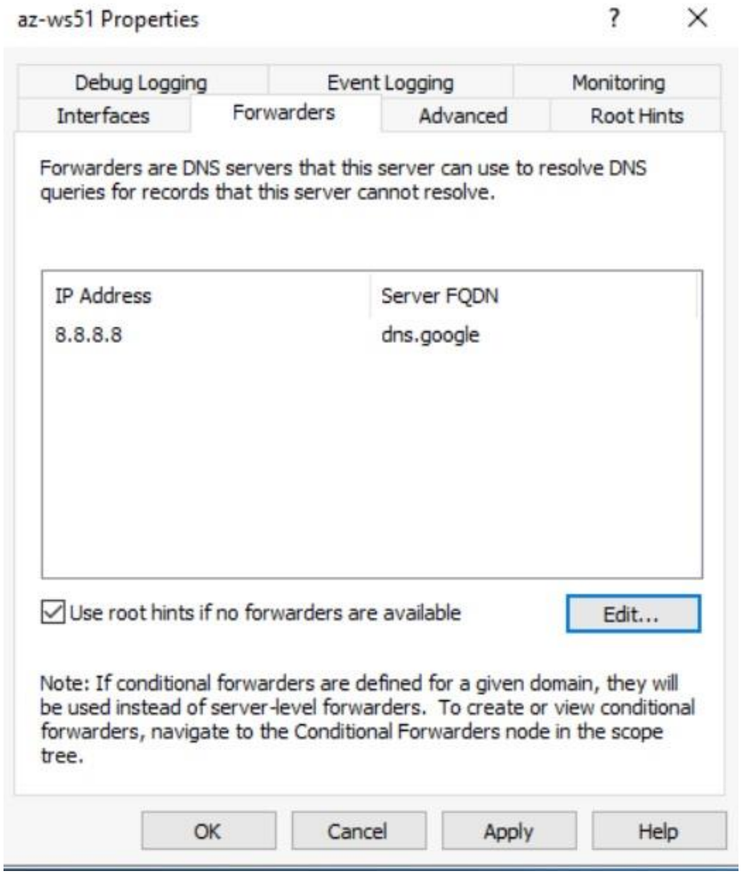
DNS Server Install (step-by-step)

To install a DNS Server on a Windows Server machine, first we need to add the DNS Server Role. One of the ways to do this is through the Server Manager GUI - Manage - Add Roles and Features.
After the installation, the DNS Manager tool will appear under the Tools menu of Server Manager. From the DNS Manager we can configure our DNS Server. First, we create a Forward Lookup Zone, named fdauti.com. Our DNS Server will be authoritative for answering DNS queries inside this zone. We proceed by creating 3 A records one for each VM in our Azure premise. This type of record will translate a host/domain name to an IP address.



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], az-ws51., hostmaster.
(same as parent folder)	Name Server (NS)	az-ws51.
az-ws51	Host (A)	172.16.51.4
az-fer51	Host (A)	10.0.51.4
iis51	Host (A)	172.16.51.4

After this step, we need to configure a DNS Forwarder, to resolve DNS quires that our DNS Server can't resolve. This would be queries related to other zones other then our configured one, fdauti.com



Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

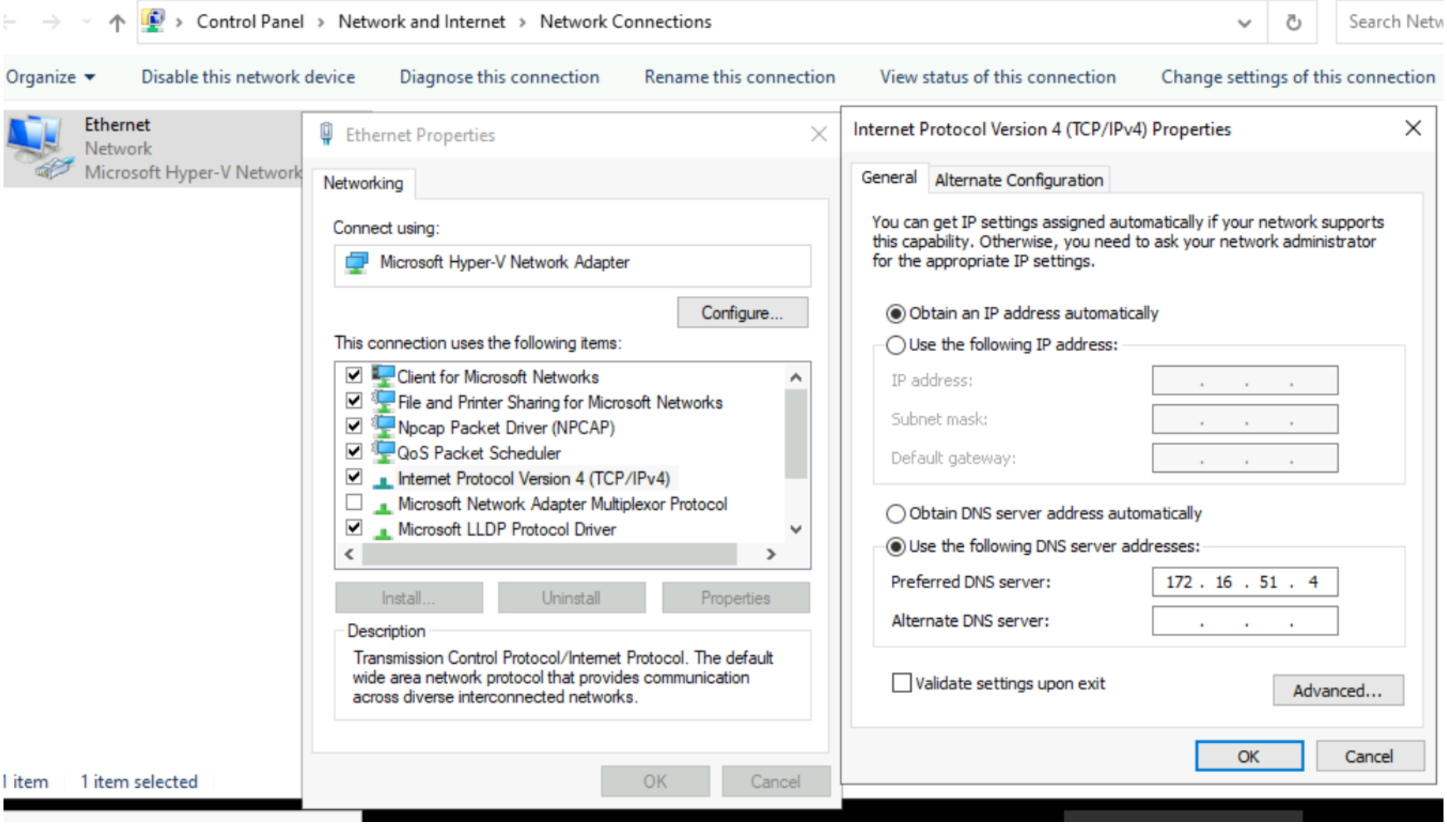
IP Address	Server FQDN
8.8.8.8	dns.google

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

This can be done on the az-ws51 properties of our DNS Server, as shown in this image. In this example, we are using the Google public DNS Server address of 8.8.8.8

After configuring the DNS Server on az-ws51, we need to make sure that our clients are using the DNS Server configured above to resolve queries. This can be done in the TCP/IP Properties of the Network Adapter on our az-wc51 VM, specifying as preferred DNS Server the IP of our az-ws51 VM.


Control Panel › Network and Internet › Network Connections
Search Netw
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet
Network
Microsoft Hyper-V Network
1 item
1 item selected
Ethernet Properties
Networking

Connect using:
Microsoft Hyper-V Network Adapter
Configure...

This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Npcap Packet Driver (NPCAP)
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

Install... Uninstall Properties

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

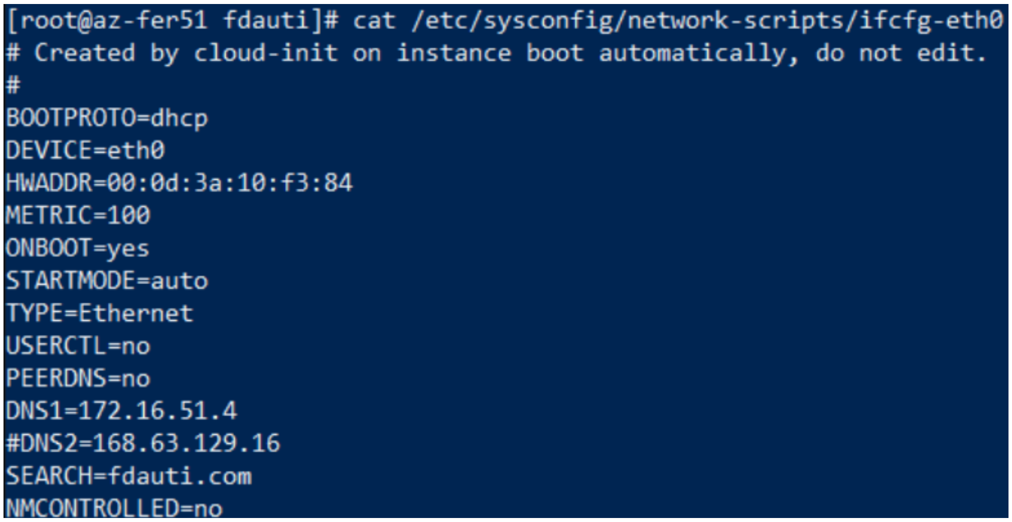
● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 172 . 16 . 51 . 4
Alternate DNS server: . . .

□ Validate settings upon exit

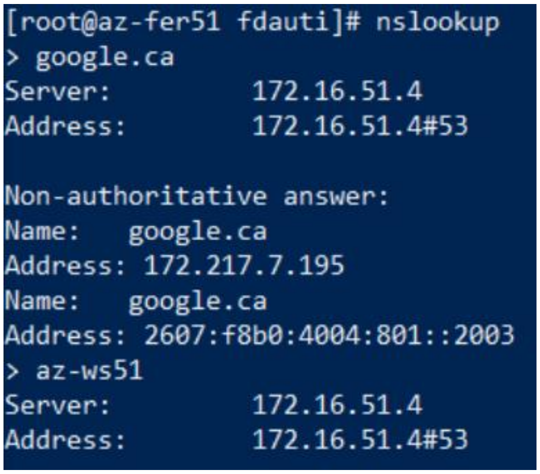
On the az-ws51 itself, we can set the Preferred DNS server as 127.0.0.1

On the az-fer51 VM, this can be done by editing the configuration file of the network interface, as shown below, adding the az-ws51 IP as the dns server, a SEARCH parameter when not using FQDNs for queries and NMCONTROLLED set to no, to avoid resetting of config by the network manager service, and a PEERDNS option set to no - since we are using DHCP on this interface.



```
[root@az-fer51 fdauti]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
HWADDR=00:0d:3a:10:f3:84
METRIC=100
ONBOOT=yes
STARTMODE=auto
TYPE=Ethernet
USERCTL=no
PEERDNS=no
DNS1=172.16.51.4
#DNS2=168.63.129.16
SEARCH=fdauti.com
NMCONTROLLED=no
```

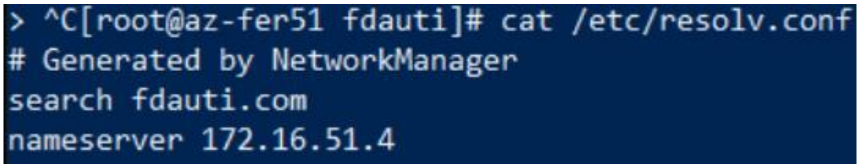
Queries would be resolved like shown below:



```
[root@az-fer51 fdauti]# nslookup
> google.ca
Server:         172.16.51.4
Address:        172.16.51.4#53

Non-authoritative answer:
Name:   google.ca
Address: 172.217.7.195
Name:   google.ca
Address: 2607:f8b0:4004:801::2003
> az-ws51
Server:         172.16.51.4
Address:        172.16.51.4#53
```

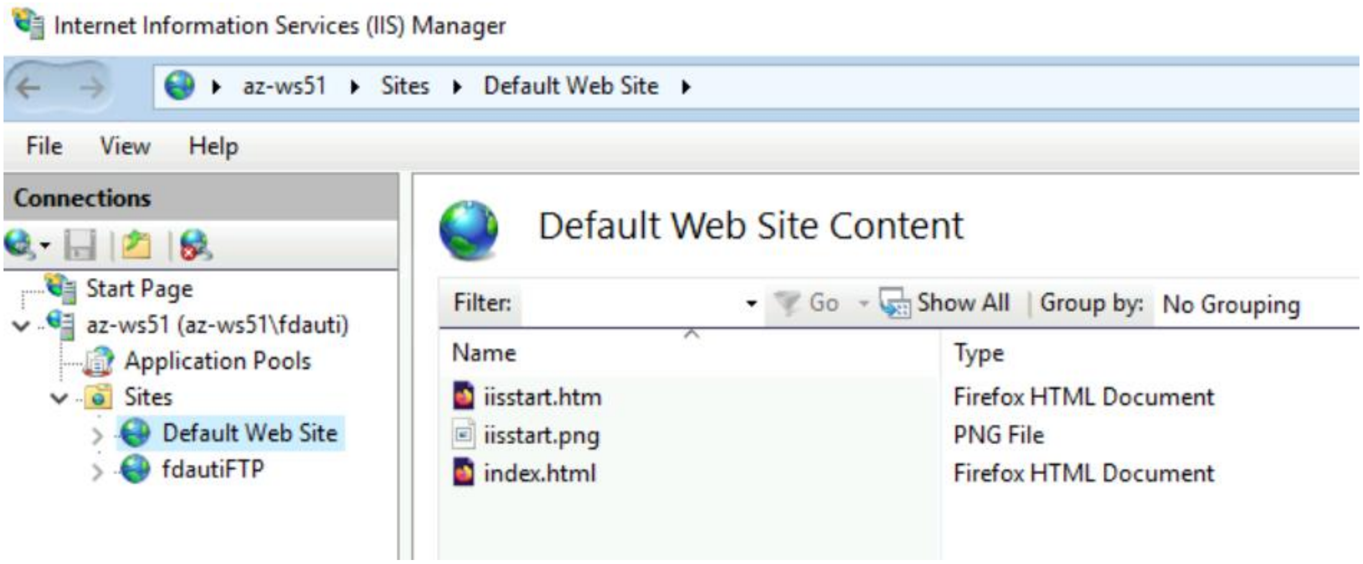
After the above configurations, the /etc/reslov.conf file would look like:



```
> ^C[root@az-fer51 fdauti]# cat /etc/resolv.conf
# Generated by NetworkManager
search fdauti.com
nameserver 172.16.51.4
```

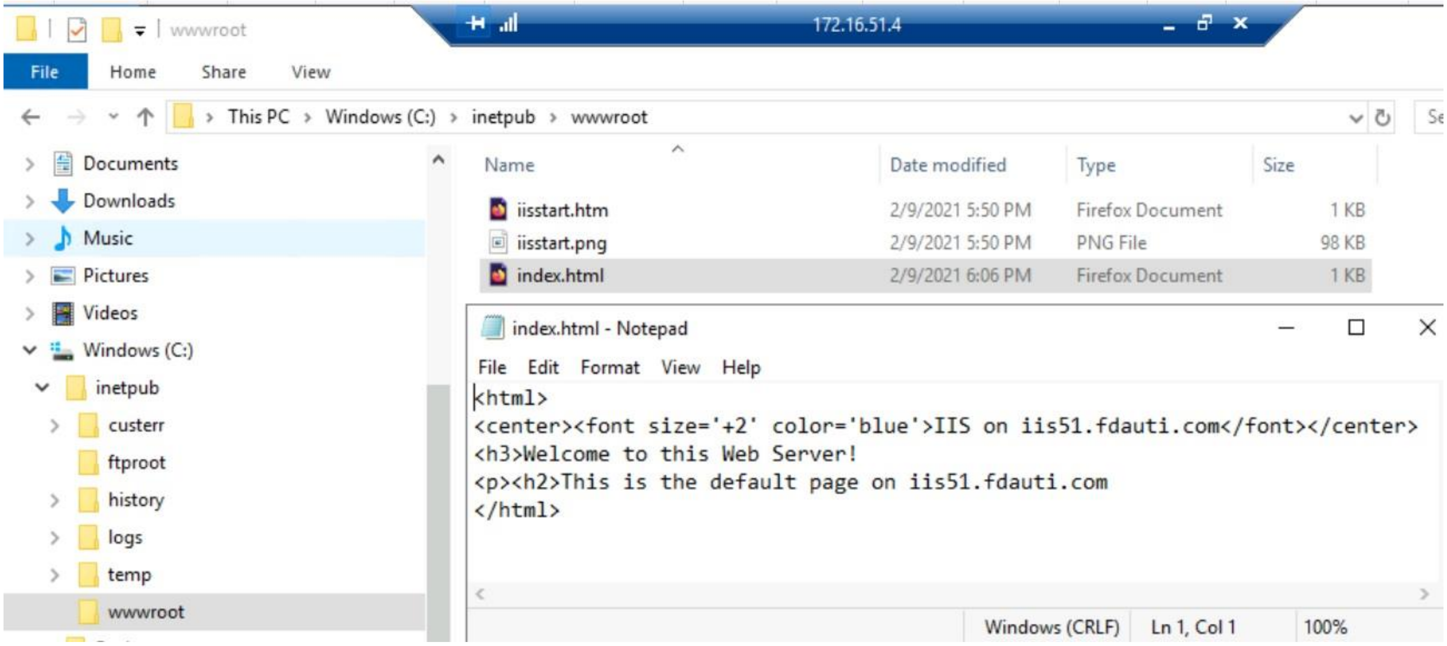
IIS Install (step-by-step)

First, we need to install the Web Server role by using the Server Manager GUI under Add Roles and Features. The IIS Server is configured using the IIS Manager tool. We can edit the Default Web Site or add new ones. By default, the server will listen for connections on port 80. We can add an index.html file to be shown by default when lending on the main page of the site. The order of priority for the files can be specified under the Default Document option inside Default Web Site.



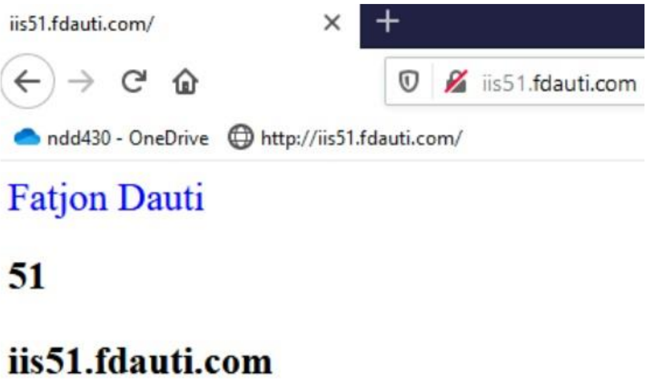
Name	Type
iisstart.htm	Firefox HTML Document
iisstart.png	PNG File
index.html	Firefox HTML Document

The content of our index.html file, created statically through html code and placed under the IIS root directory, will look like:



Name	Date modified	Type	Size
iisstart.htm	2/9/2021 5:50 PM	Firefox Document	1 KB
iisstart.png	2/9/2021 5:50 PM	PNG File	98 KB
index.html	2/9/2021 6:06 PM	Firefox Document	1 KB

```
<html>
<center><font size='+2' color='blue'>IIS on iis51.fdauti.com</font></center>
<h3>Welcome to this Web Server!
<p><h2>This is the default page on iis51.fdauti.com
</html>
```



Fatjon Dauti

51

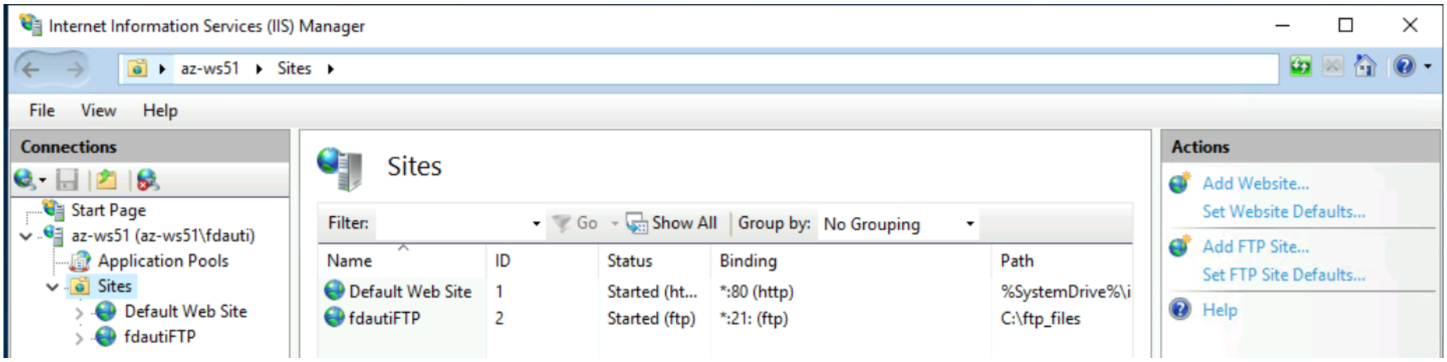
iis51.fdauti.com

Browsing the iis51.fdauti.com website address!

FTP Server Install (step-by-step)

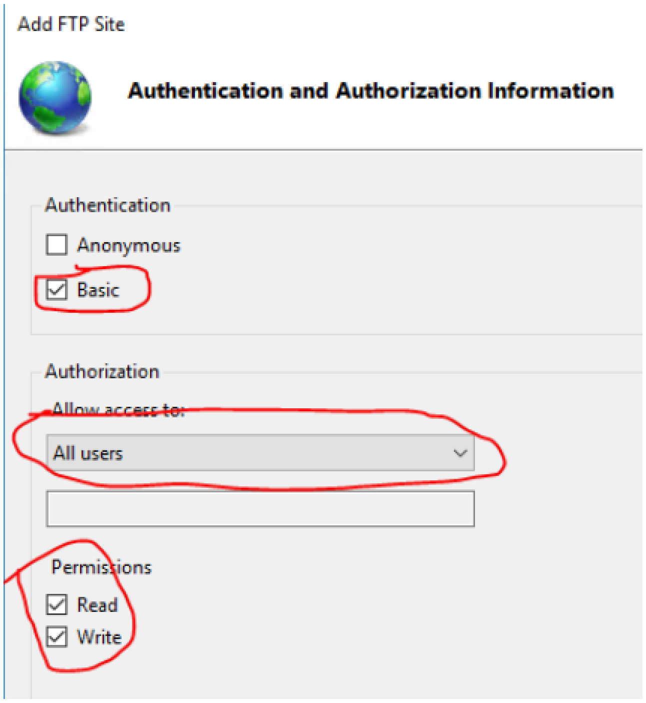
- **Include the ports used for the service and the procedure to open the correct ports in Windows Firewall**

To run a FTP Server under Windows Server, we need to install the FTP Server role under the Web Server role using Server Manager GUI. Using IIS Manager tool we can add an FTP Site under Sites, specifying the default path for the files, for instance, C:\ftp_files\



Name	ID	Status	Binding	Path
Default Web Site	1	Started (ht...	*:80 (http)	%SystemDrive%\i
fdautiFTP	2	Started (ftp)	*:21: (ftp)	C:\ftp_files

For our demonstration purpose, when creating the ftp site, we can specify the options of not using SSL encryption with Basic Authentication and allow access to the ftp site to All Users of this Windows Server, with read and write permissions.


Add FTP Site

Authentication and Authorization Information

Authentication

☐ Anonymous

☑ Basic

Authorization

Allow access to:

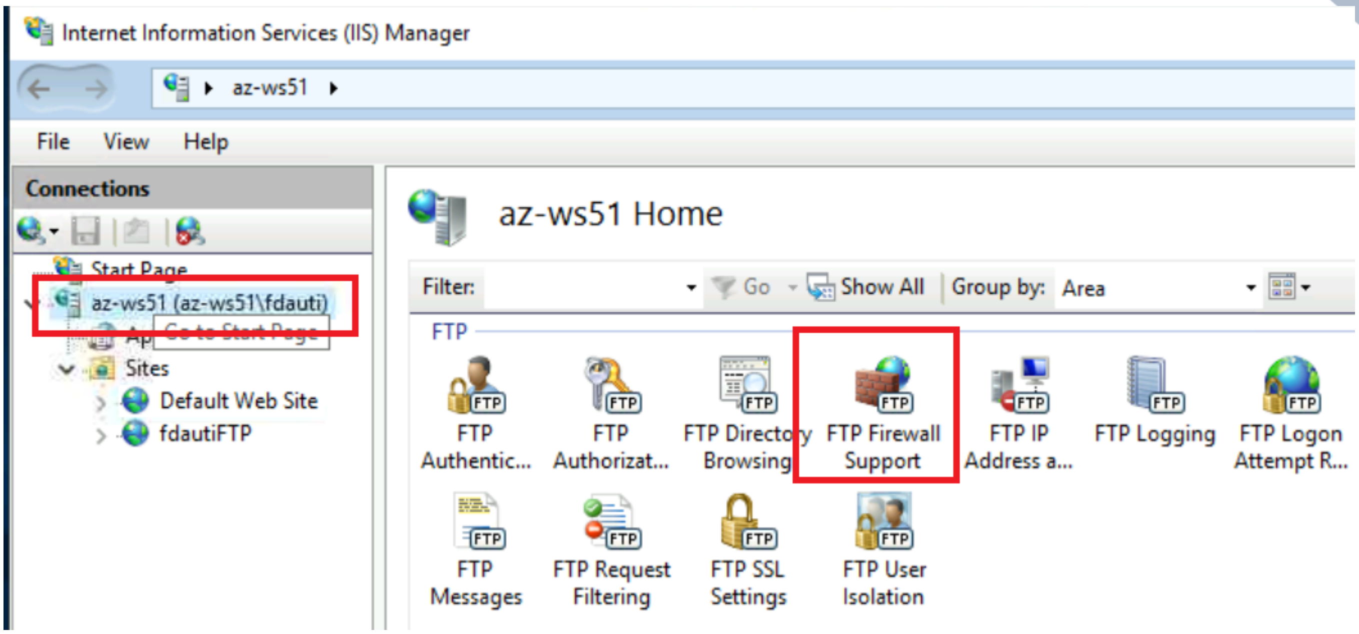
All users

Permissions

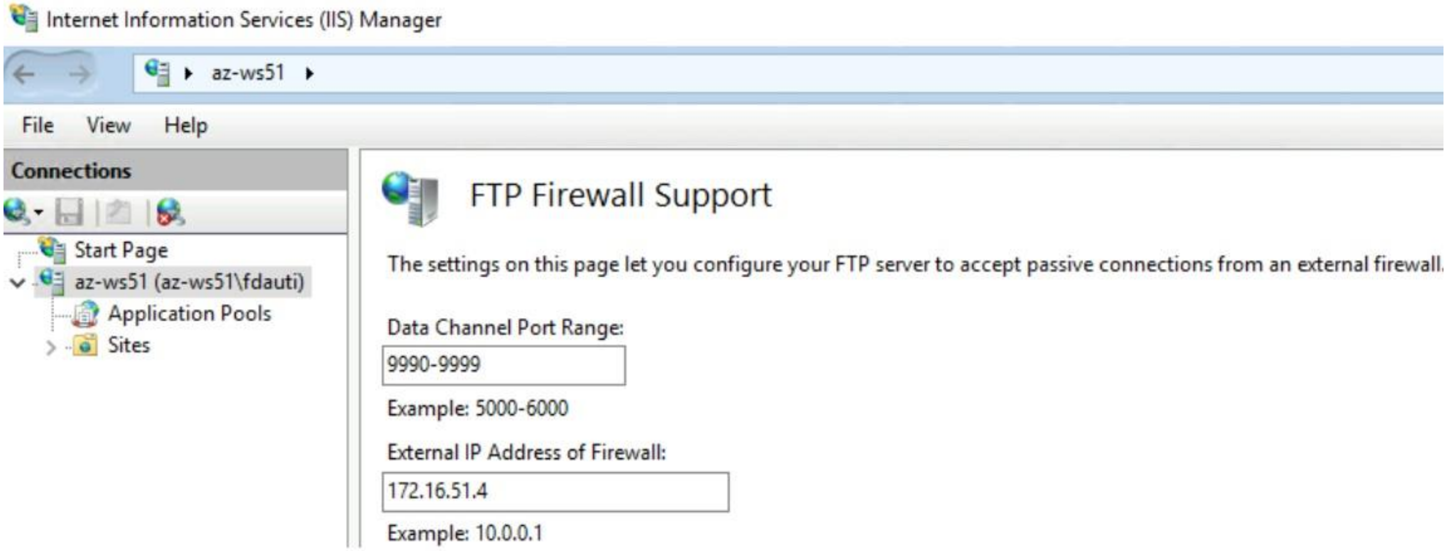
☑ Read

☑ Write

Next step is to configure the FTP Firewall Support under the as-ws51 server shown inside Connections pane of IIS Manager.



Passive FTP connections for ftp-data transfer allowed on ports range 9990-9999, configured on ISS Manager. To make configuration changes effective we need to restart the FTPSVC Service under Task Manager.



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

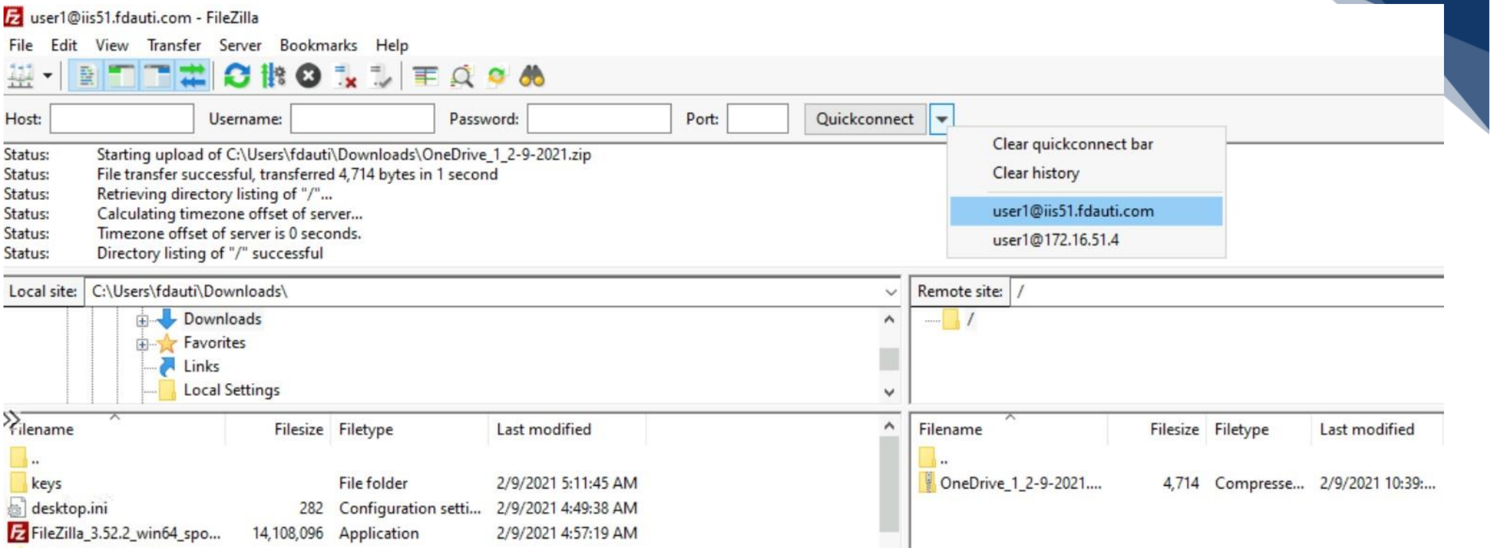
Data Channel Port Range: 9990-9999

Example: 5000-6000

External IP Address of Firewall: 172.16.51.4

Example: 10.0.0.1

We can verify functionality of the FTP Server by login through an FTP Client like FileZilla on the az-wc51 machine, using the ***user1*** user account created on az-ws51 for this purpose. The user can browse and upload files to the server.



Host: Username: Password: Port:

```
Status:     Starting upload of C:\Users\fdauti\Downloads\OneDrive_1_2-9-2021.zip
Status:     File transfer successful, transferred 4,714 bytes in 1 second
Status:     Retrieving directory listing of "/"...
Status:     Calculating timezone offset of server...
Status:     Timezone offset of server is 0 seconds.
Status:     Directory listing of "/" successful
```

Local site: C:\Users\fdauti\Downloads\

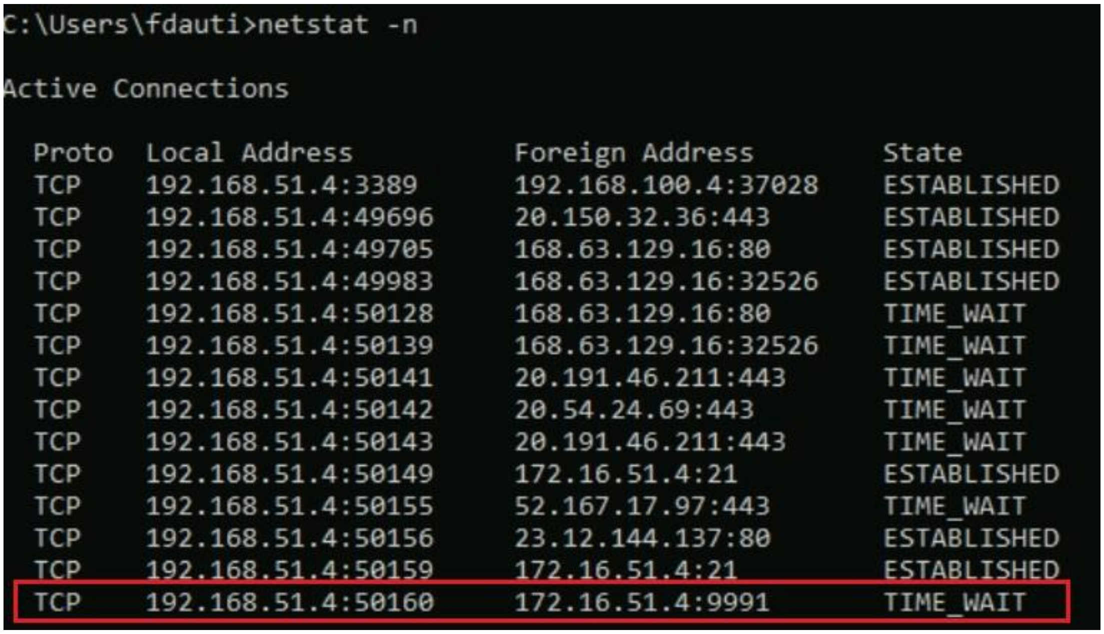
- Downloads
- Favorites
- Links
- Local Settings

Filename	Filesize	Filetype	Last modified
..			
keys		File folder	2/9/2021 5:11:45 AM
desktop.ini	282	Configuration setti...	2/9/2021 4:49:38 AM
FileZilla_3.52.2_win64_spo...	14,108,096	Application	2/9/2021 4:57:19 AM

Remote site: /

Filename	Filesize	Filetype	Last modified
..			
OneDrive_1_2-9-2021....	4,714	Compresse...	2/9/2021 10:39:...

Running netstat, we see the connection being established on 9991 port, which is under the allowed port range, when a file transfer begins.



```
C:\Users\fdauti>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.51.4:3389      192.168.100.4:37028    ESTABLISHED
  TCP    192.168.51.4:49696     20.150.32.36:443       ESTABLISHED
  TCP    192.168.51.4:49705     168.63.129.16:80       ESTABLISHED
  TCP    192.168.51.4:49983     168.63.129.16:32526    ESTABLISHED
  TCP    192.168.51.4:50128     168.63.129.16:80       TIME_WAIT
  TCP    192.168.51.4:50139     168.63.129.16:32526    TIME_WAIT
  TCP    192.168.51.4:50141     20.191.46.211:443      TIME_WAIT
  TCP    192.168.51.4:50142     20.54.24.69:443        TIME_WAIT
  TCP    192.168.51.4:50143     20.191.46.211:443      TIME_WAIT
  TCP    192.168.51.4:50149     172.16.51.4:21         ESTABLISHED
  TCP    192.168.51.4:50155     52.167.17.97:443       TIME_WAIT
  TCP    192.168.51.4:50156     23.12.144.137:80       ESTABLISHED
  TCP    192.168.51.4:50159     172.16.51.4:21         ESTABLISHED
  TCP    192.168.51.4:50160     172.16.51.4:9991       TIME_WAIT
```

Appendix A – DNS Settings

DNS Table

- **Expand this table to include all FQDNs and IPs configured in your DNS**

FQDN	IP Address
az-wc51.fdauti.com	192.168.51.4
az-fer51.fdauti.com	10.0.51.4
ws51.fdauti.com	172.16.51.4

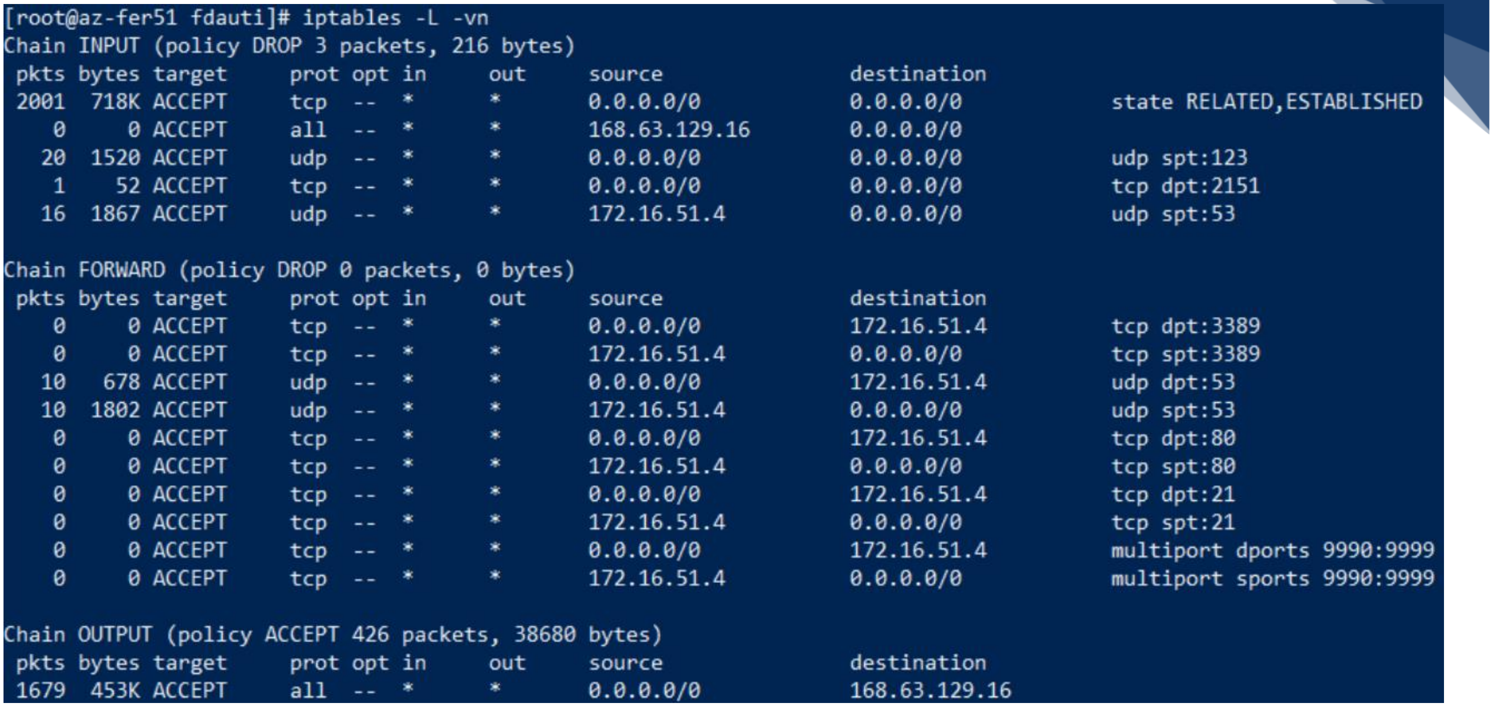
Appendix B – Firewall Configurations

- **iptables Configurations for az-fer51**

In the configuration below, we are allowing SSH traffic on tcp destination port 2151 and DNS traffic originating from DNS Server 172.16.51.4 on udp port 53. Port 123 is used by the Network Time Protocol (NTP) for time synchronization.

IP Forwarding should be enabled on az-fer51, the same it was as done on onprem-R VM on checkpoint 1. It is recommended to apply firewall configurations step by step, after establishing full connectivity for the services first, and never apply the rules permanently before confirming they are working as intended. A reboot of the az-fer51 VM or iptables service will flush non saved rules.

The IP addres 168.63.129.16 on iptables, is the Azure public address that acts as the default gateway on the external interface for the VMs.



```
[root@az-fer51 fdauti]# iptables -L -vn
Chain INPUT (policy DROP 3 packets, 216 bytes)
 pkts bytes target     prot opt in     out     source               destination
 2001  718K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  *      *       168.63.129.16        0.0.0.0/0
   20  1520 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:123
    1    52 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2151
   16  1867 ACCEPT     udp  --  *      *       172.16.51.4          0.0.0.0/0            udp spt:53

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          tcp dpt:3389
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            tcp spt:3389
   10   678 ACCEPT     udp  --  *      *       0.0.0.0/0            172.16.51.4          udp dpt:53
   10  1802 ACCEPT     udp  --  *      *       172.16.51.4          0.0.0.0/0            udp spt:53
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            tcp spt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            tcp spt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.51.4          multiport dports 9990:9999
    0     0 ACCEPT     tcp  --  *      *       172.16.51.4          0.0.0.0/0            multiport sports 9990:9999

Chain OUTPUT (policy ACCEPT 426 packets, 38680 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1679  453K ACCEPT     all  --  *      *       0.0.0.0/0            168.63.129.16
```

Firewall Configuration for az-ws51

On the Forward chain of iptables, we are allowing traffic related to RDP (for remote desktop connections) on port 3389, DNS Server on port 53, IIS Web Server on port 80, FTP Server control data on port 21 and transfer data on ports 9990 to 9999. Apart from DNS which uses UDP as transport protocol, the other services will use TCP. These rules are applied on the Forward chain of iptables on az-fer51, because neither the source nor the destination address inside these packet doesn't match a router's interface, so they are routed between az-wc51 and az-ws51 machines.

The configurations for the Forward Chain that apply to az-ws51 are shown in previous section. The FTP Firewall configuration for az-ws51 were explained under the FTP Server installation section.

Include here the rules you had to add to allow the FTP traffic

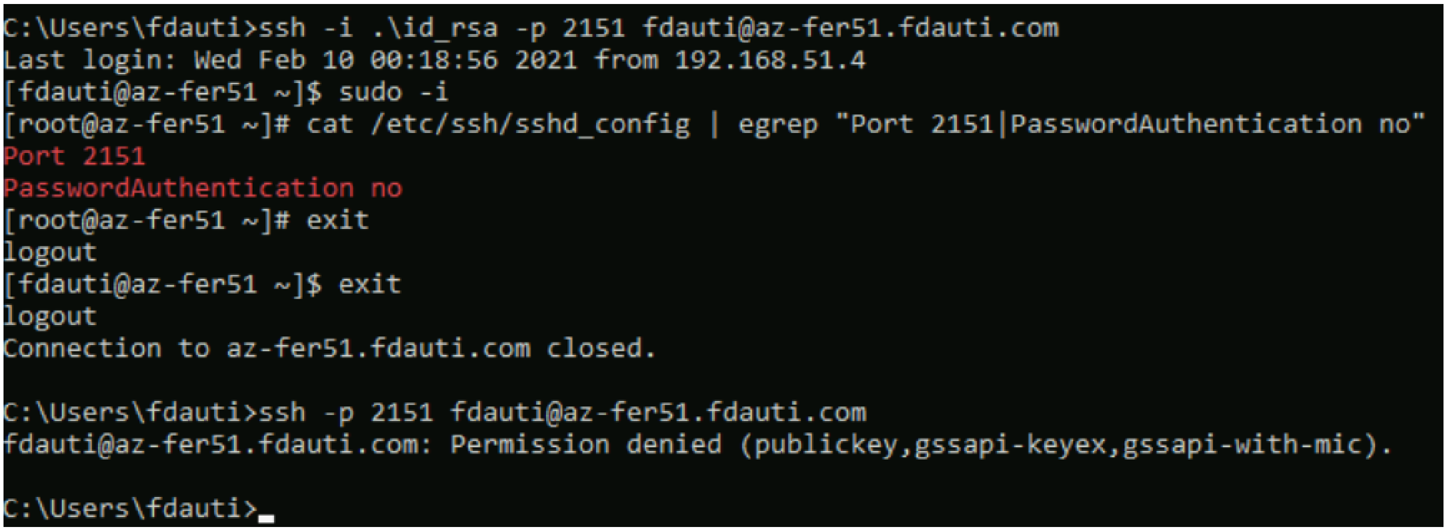
We need to apply the following rules on the FORWARD Chain of iptables in az-fer51 VM

```
iptables -A FORWARD -p tcp -d 172.16.51.4 --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.51.4 --sport 21 -j ACCEPT
iptables -A FORWARD -p tcp -d 172.16.51.4 -m multiport --dports 9990:9999 -j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.51.4 -m multiport --sports 9990:9999 -j ACCEPT
```

Appendix C – SSHD_CONF configurations

- **Include here proof of disabling password access and changes from standard to non-standard ports**

In the demonstration below, if the private key is removed from .ssh directory of user account in az-wc51, login will be denied, until we specify the private key location with -i
On ssh configuration file sshd_config in az-fer51, the Port and PasswordAuthentication option should be set as follow. To apply configurations we need to reload the service, *service sshd reload*

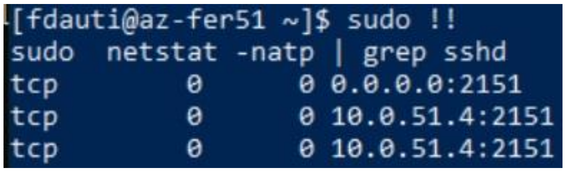


```
C:\Users\fdauti>ssh -i .\id_rsa -p 2151 fdauti@az-fer51.fdauti.com
Last login: Wed Feb 10 00:18:56 2021 from 192.168.51.4
[fdauti@az-fer51 ~]$ sudo -i
[root@az-fer51 ~]# cat /etc/ssh/sshd_config | egrep "Port 2151|PasswordAuthentication no"
Port 2151
PasswordAuthentication no
[root@az-fer51 ~]# exit
logout
[fdauti@az-fer51 ~]$ exit
logout
Connection to az-fer51.fdauti.com closed.

C:\Users\fdauti>ssh -p 2151 fdauti@az-fer51.fdauti.com
fdauti@az-fer51.fdauti.com: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

C:\Users\fdauti>_
```

The ssh service is listing on the new port specified in sshd_config



```
[fdauti@az-fer51 ~]$ sudo !!
sudo  netstat -natp | grep sshd
tcp        0      0 0.0.0.0:2151
tcp        0      0 10.0.51.4:2151
tcp        0      0 10.0.51.4:2151
```

References

https://medium.com/@JohGeoCoder/allowing-ftp-access-on-windows-server-2016-hosted-on-microsoft-azure-af25898df958
https://computingforgeeks.com/how-to-configure-default-site-in-iis-server/
https://linux.die.net/man/8/iptables