

Networks Worksheet 4

Task 1: Utilizing ARP and Routing Tables

Figure 1 Server 1 ARP table

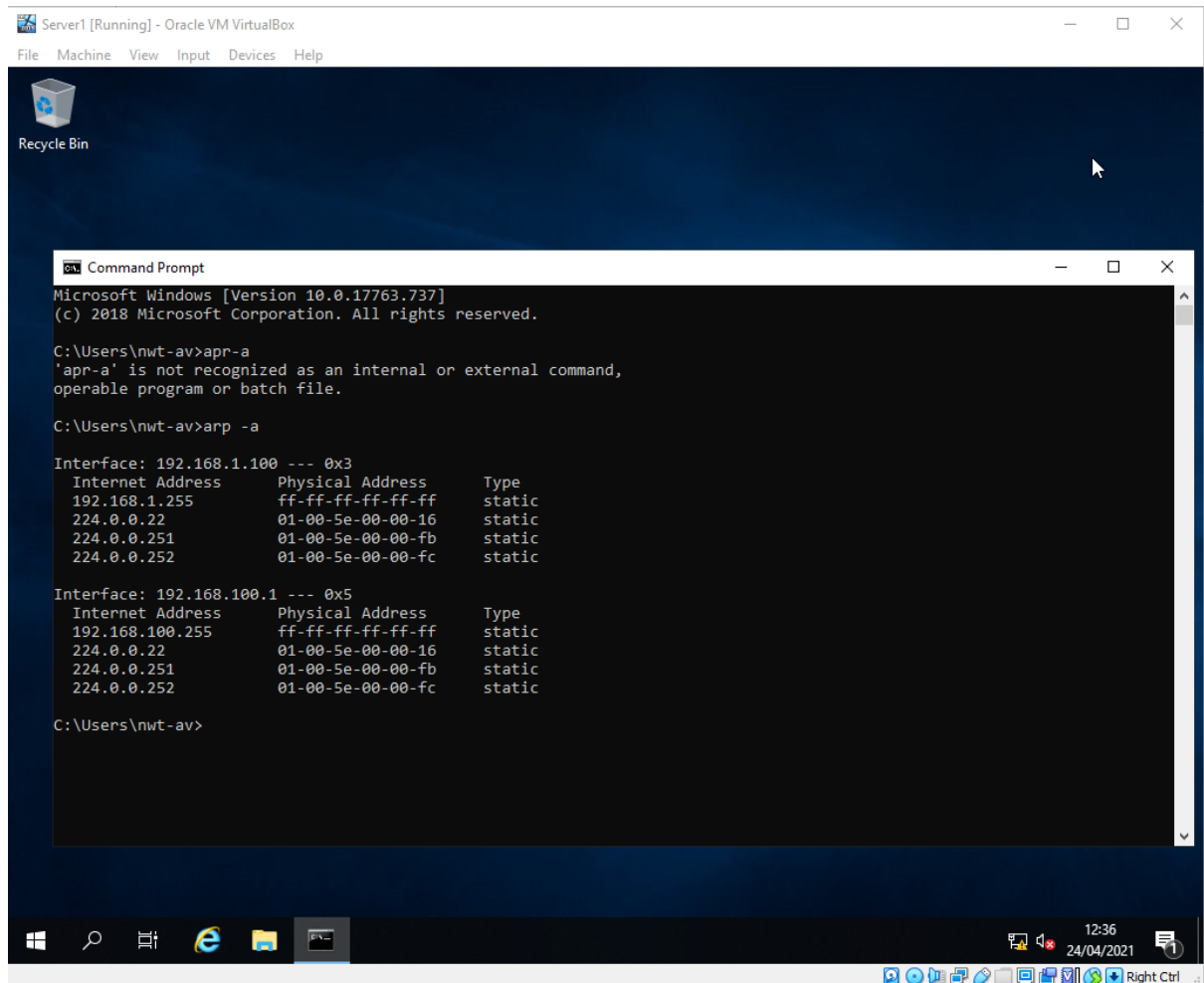
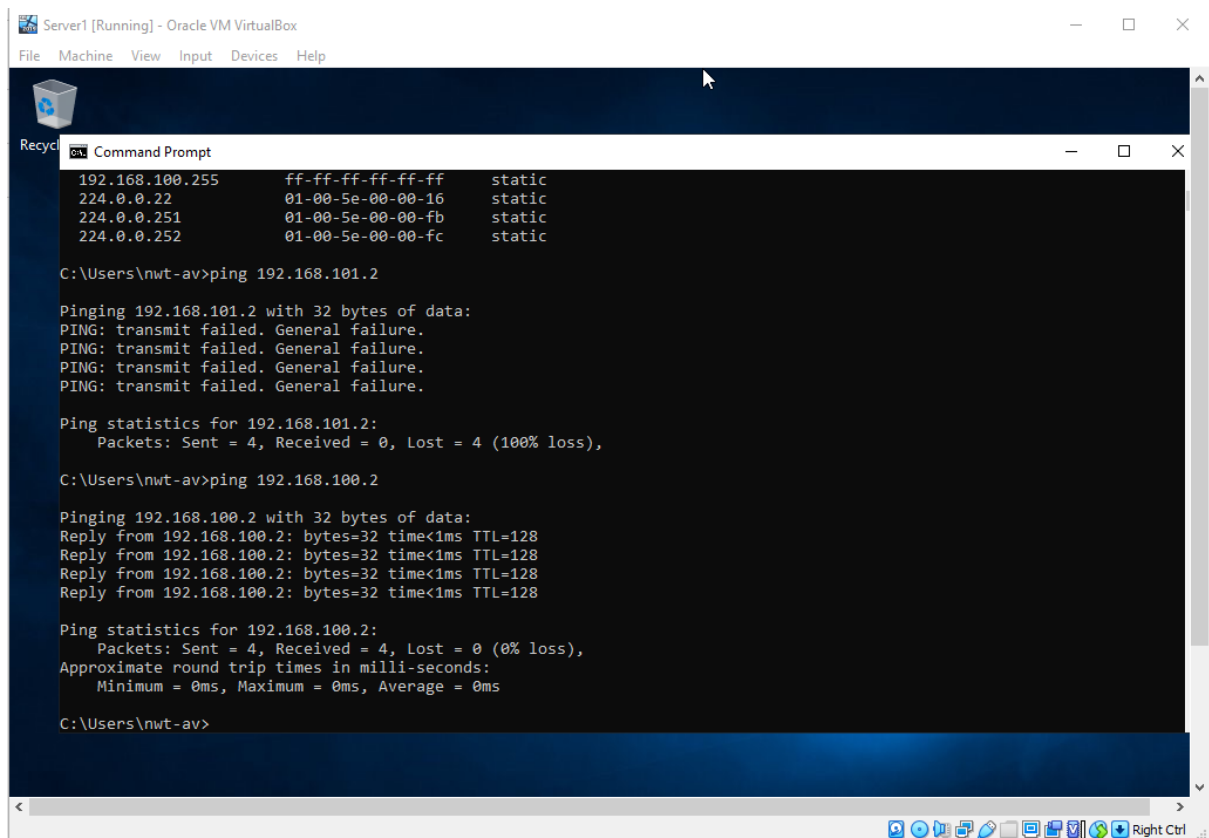


Figure 2 Server 1 can successfully ping client 1



The screenshot shows a Windows Command Prompt window titled "Server1 [Running] - Oracle VM VirtualBox". The window displays the following text:

```
192.168.100.255      ff-ff-ff-ff-ff-ff      static
224.0.0.22          01-00-5e-00-00-16      static
224.0.0.251         01-00-5e-00-00-fb      static
224.0.0.252         01-00-5e-00-00-fc      static

C:\Users\nwt-av>ping 192.168.101.2

Pinging 192.168.101.2 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.101.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\nwt-av>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128
Reply from 192.168.100.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nwt-av>
```

The window also shows a taskbar at the bottom with various icons and the text "Right Ctrl".

Figure 3 server 2 can successfully ping client 2

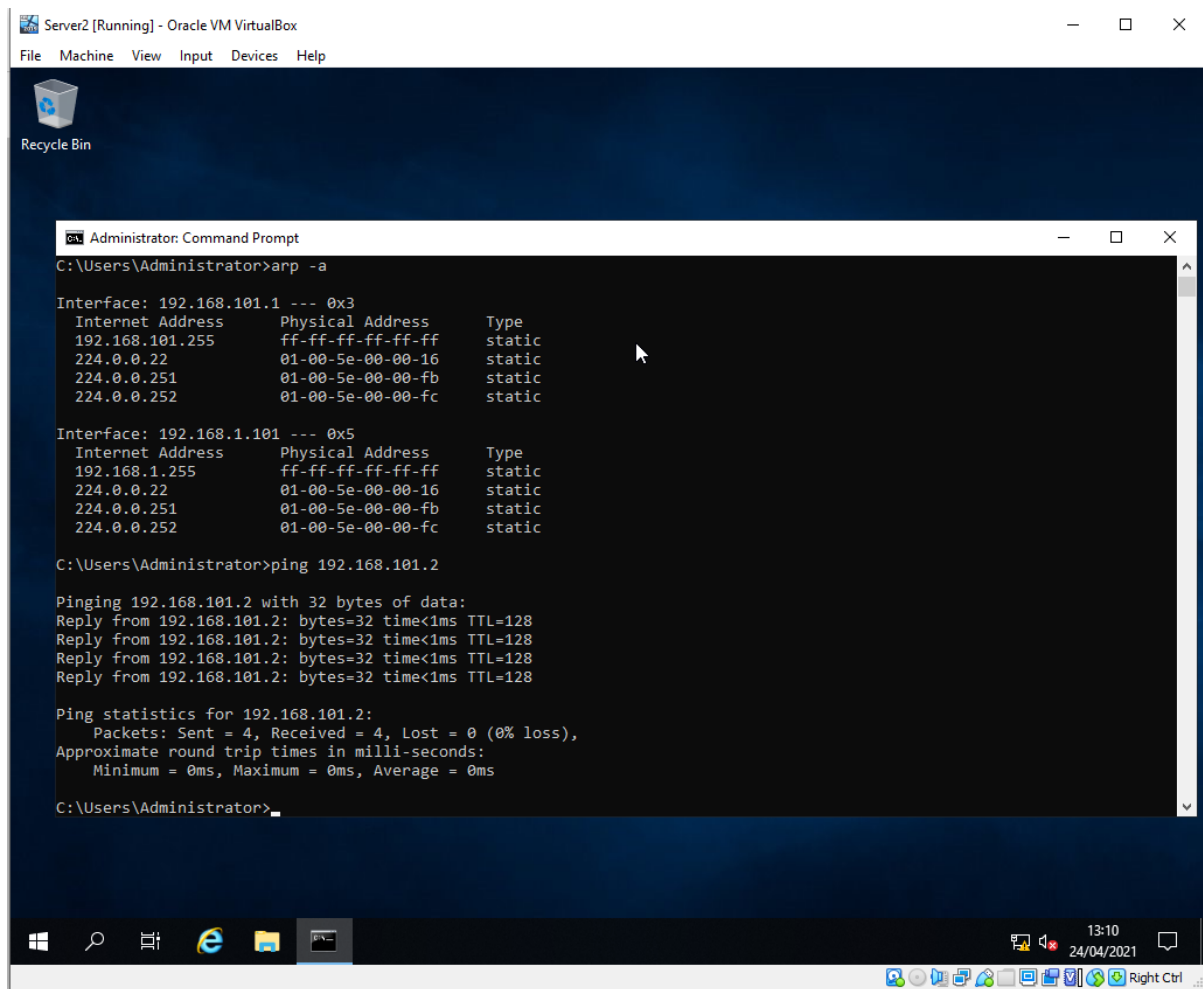
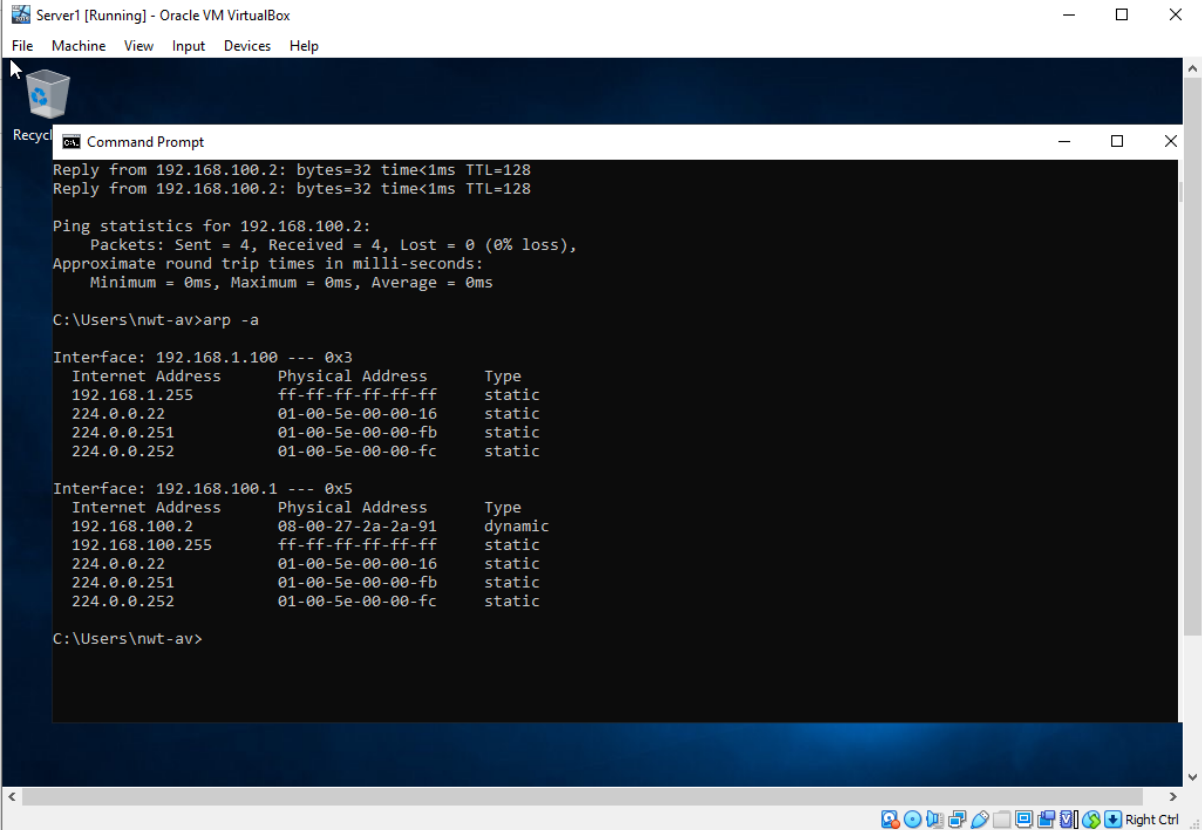


Figure 4 ARP table updated with new connection from client 1



The screenshot shows a Windows Command Prompt window titled "Server1 [Running] - Oracle VM VirtualBox". The window displays the following text:

```
Recycle Bin
C:\Users\nwt-av>arp -a

Interface: 192.168.1.100 --- 0x3
Internet Address      Physical Address      Type
192.168.1.255          ff-ff-ff-ff-ff-ff     static
224.0.0.22             01-00-5e-00-00-16     static
224.0.0.251            01-00-5e-00-00-fb     static
224.0.0.252            01-00-5e-00-00-fc     static

Interface: 192.168.100.1 --- 0x5
Internet Address      Physical Address      Type
192.168.100.2          08-00-27-2a-2a-91     dynamic
192.168.100.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22             01-00-5e-00-00-16     static
224.0.0.251            01-00-5e-00-00-fb     static
224.0.0.252            01-00-5e-00-00-fc     static

C:\Users\nwt-av>
```

The ARP table is updated with a new connection from client 1, showing the dynamic entry for 192.168.100.2 with physical address 08-00-27-2a-2a-91.

Figure 5 Route print table on Server 1

```

Server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Recycle Bin
Command Prompt

224.0.0.251      01-00-5e-00-00-fb  static
224.0.0.252      01-00-5e-00-00-fc  static

C:\Users\nwt-av>route print

=====
Interface List
3...08 00 27 48 d4 02 .....Intel(R) PRO/1000 MT Desktop Adapter
5...08 00 27 8d db 50 .....Intel(R) PRO/1000 MT Desktop Adapter #2
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface           Metric
127.0.0.0                  255.0.0.0        On-link             127.0.0.1            331
127.0.0.1                  255.255.255.255  On-link             127.0.0.1            331
127.255.255.255           255.255.255.255  On-link             127.0.0.1            331
192.168.1.0                255.255.255.0    On-link             192.168.1.100        281
192.168.1.100             255.255.255.255  On-link             192.168.1.100        281
192.168.1.255             255.255.255.255  On-link             192.168.1.100        281
192.168.100.0             255.255.255.0    On-link             192.168.100.1        281
192.168.100.1             255.255.255.255  On-link             192.168.100.1        281
192.168.100.255           255.255.255.255  On-link             192.168.100.1        281
224.0.0.0                  240.0.0.0        On-link             127.0.0.1            331
224.0.0.0                  240.0.0.0        On-link             192.168.1.100        281
224.0.0.0                  240.0.0.0        On-link             192.168.100.1        281
255.255.255.255           255.255.255.255  On-link             127.0.0.1            331
255.255.255.255           255.255.255.255  On-link             192.168.1.100        281
255.255.255.255           255.255.255.255  On-link             192.168.100.1        281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 331 ::1/128 On-link
  
```

Task 2: Deploy core services (FTP Server)

Figure 6 Confirmed machine is VM2 for FTP set-up

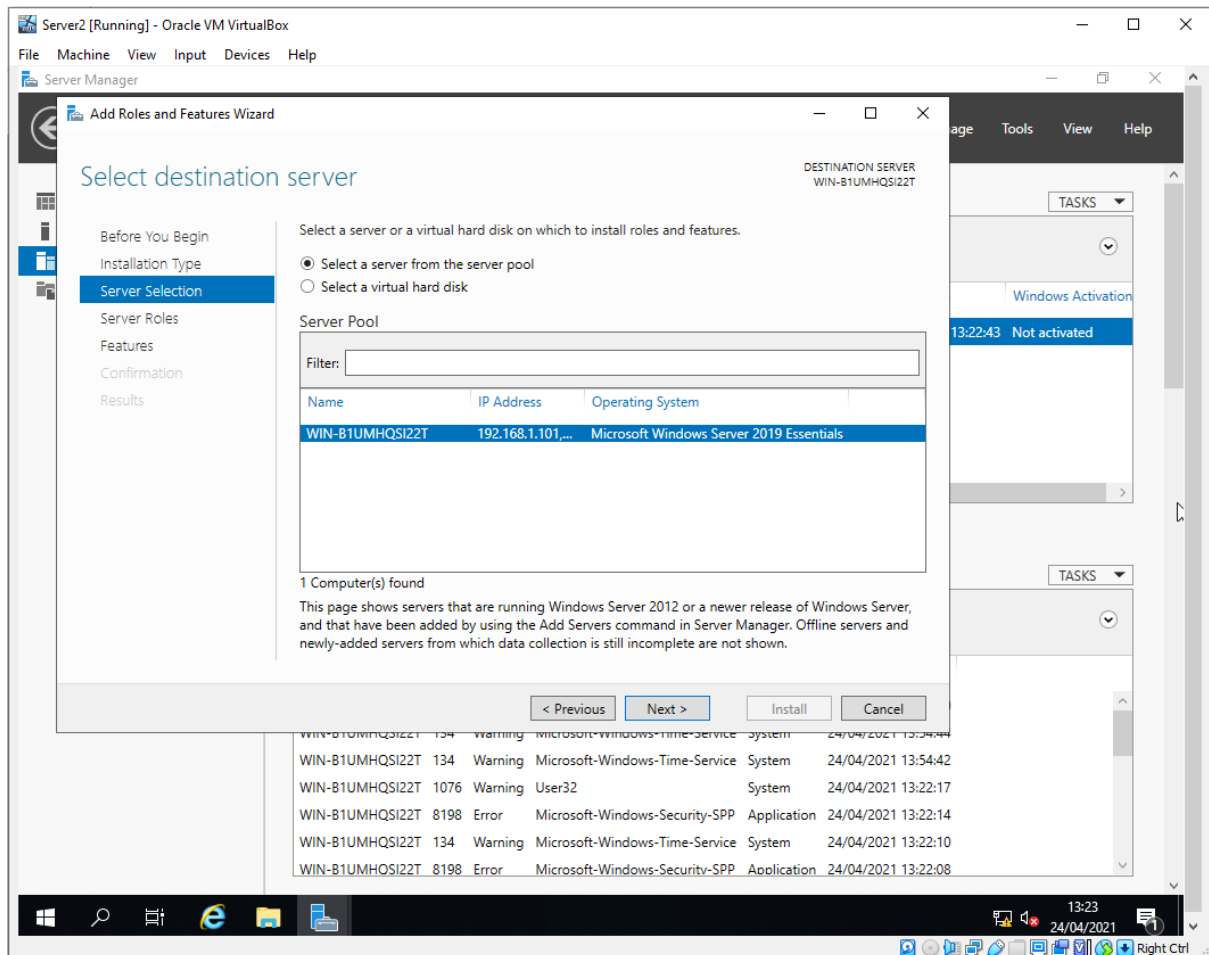


Figure 7 IIS server role selected

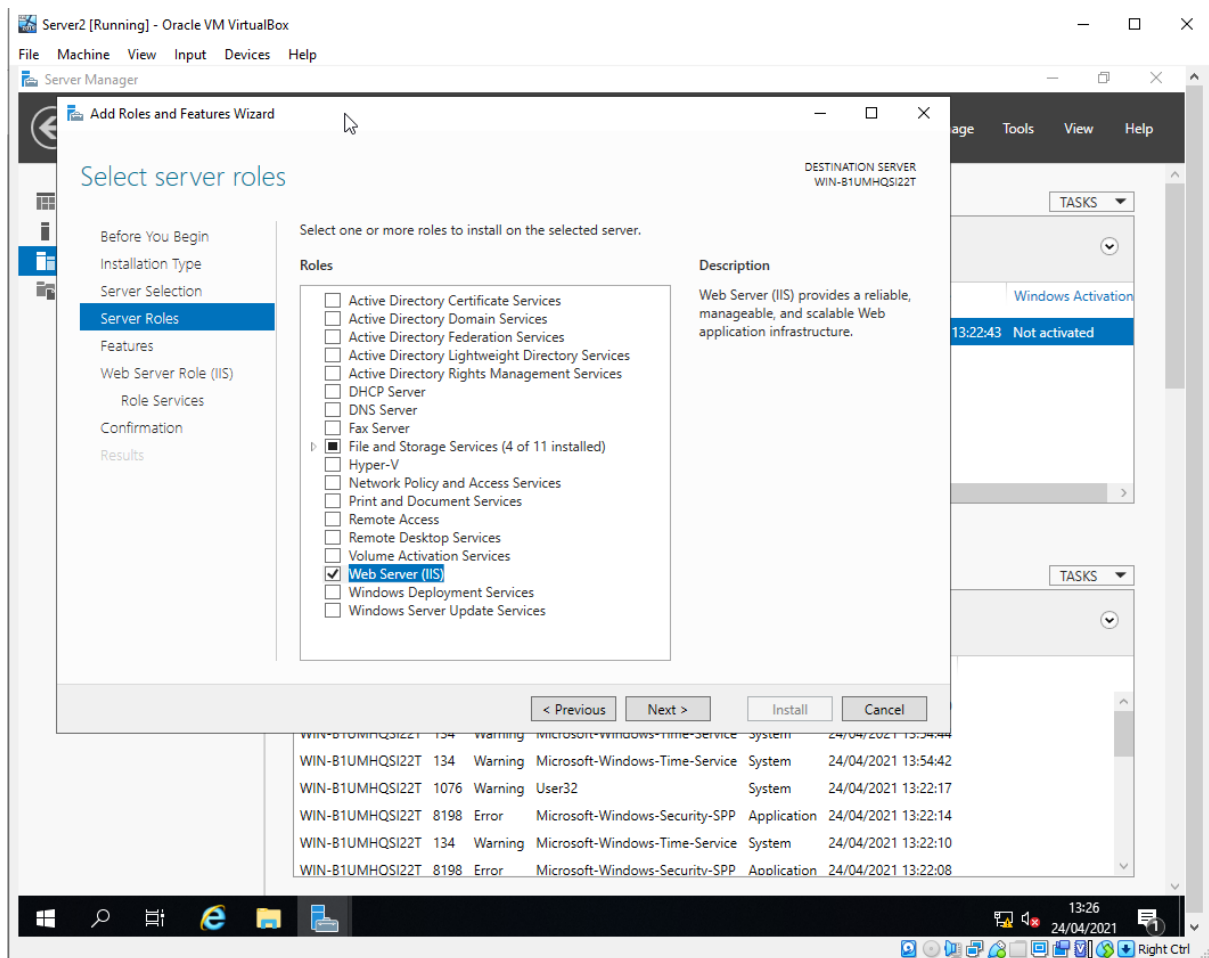


Figure 8 FTP server installed

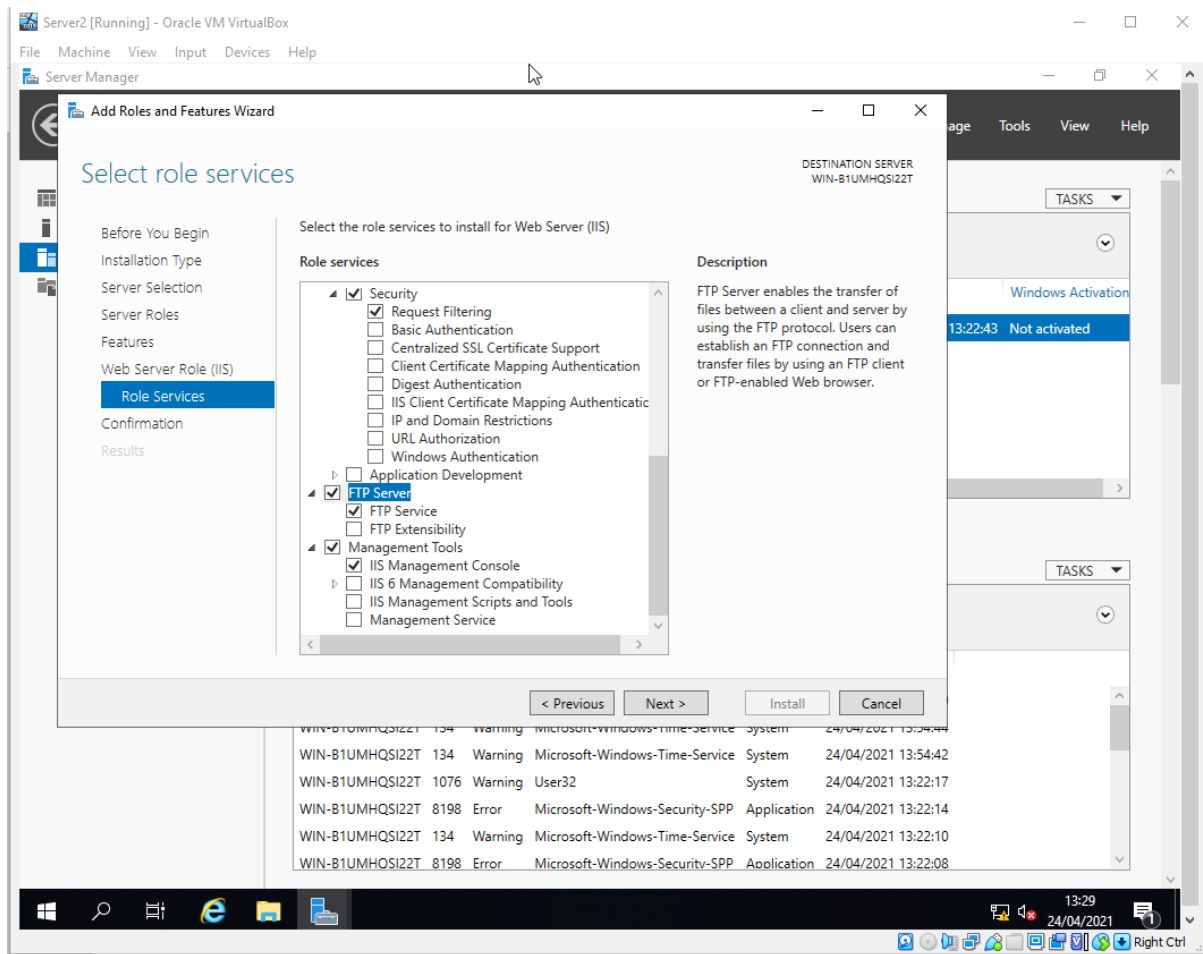


Figure 9 FTP User created

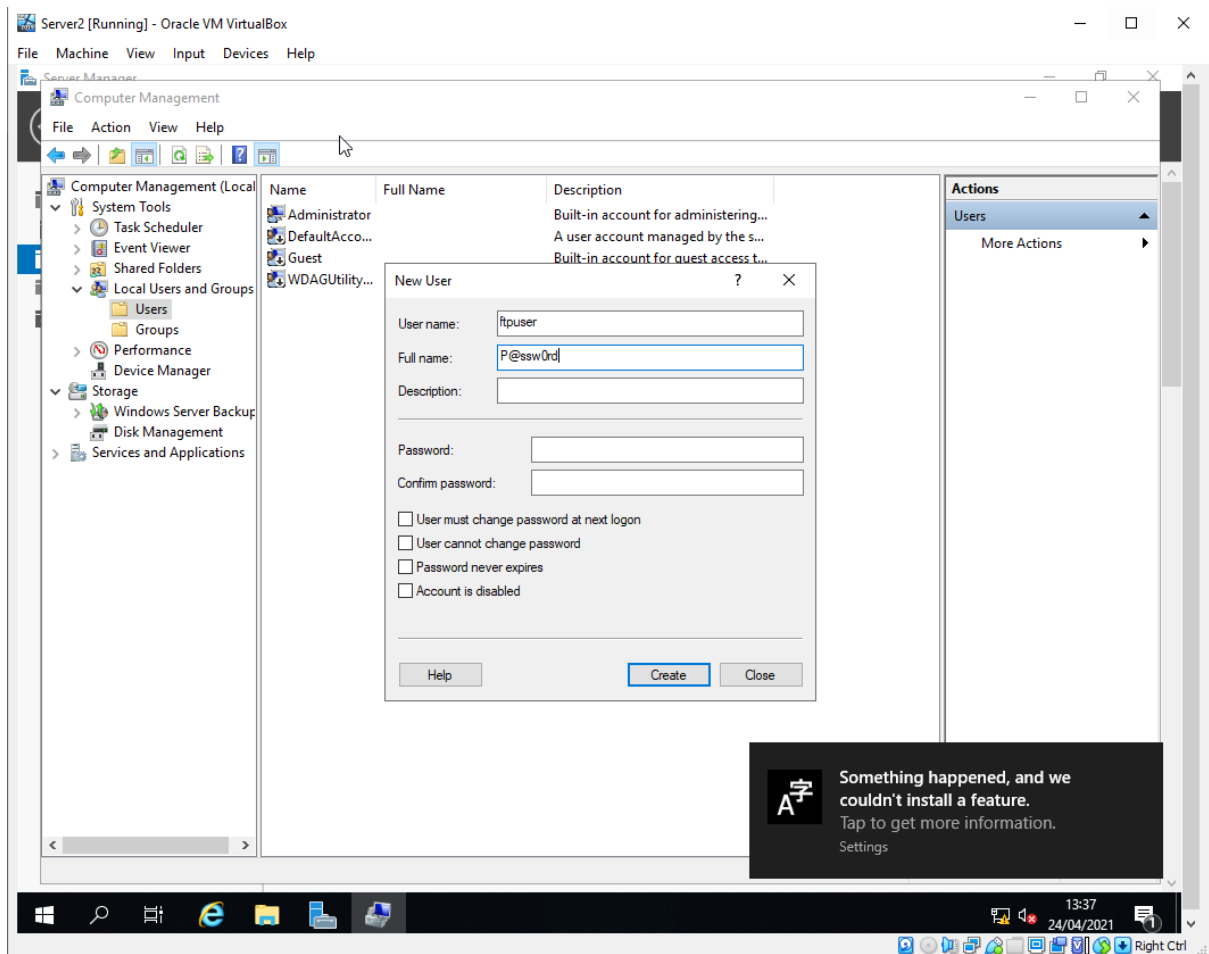


Figure 10 No SSL configured for FTP site

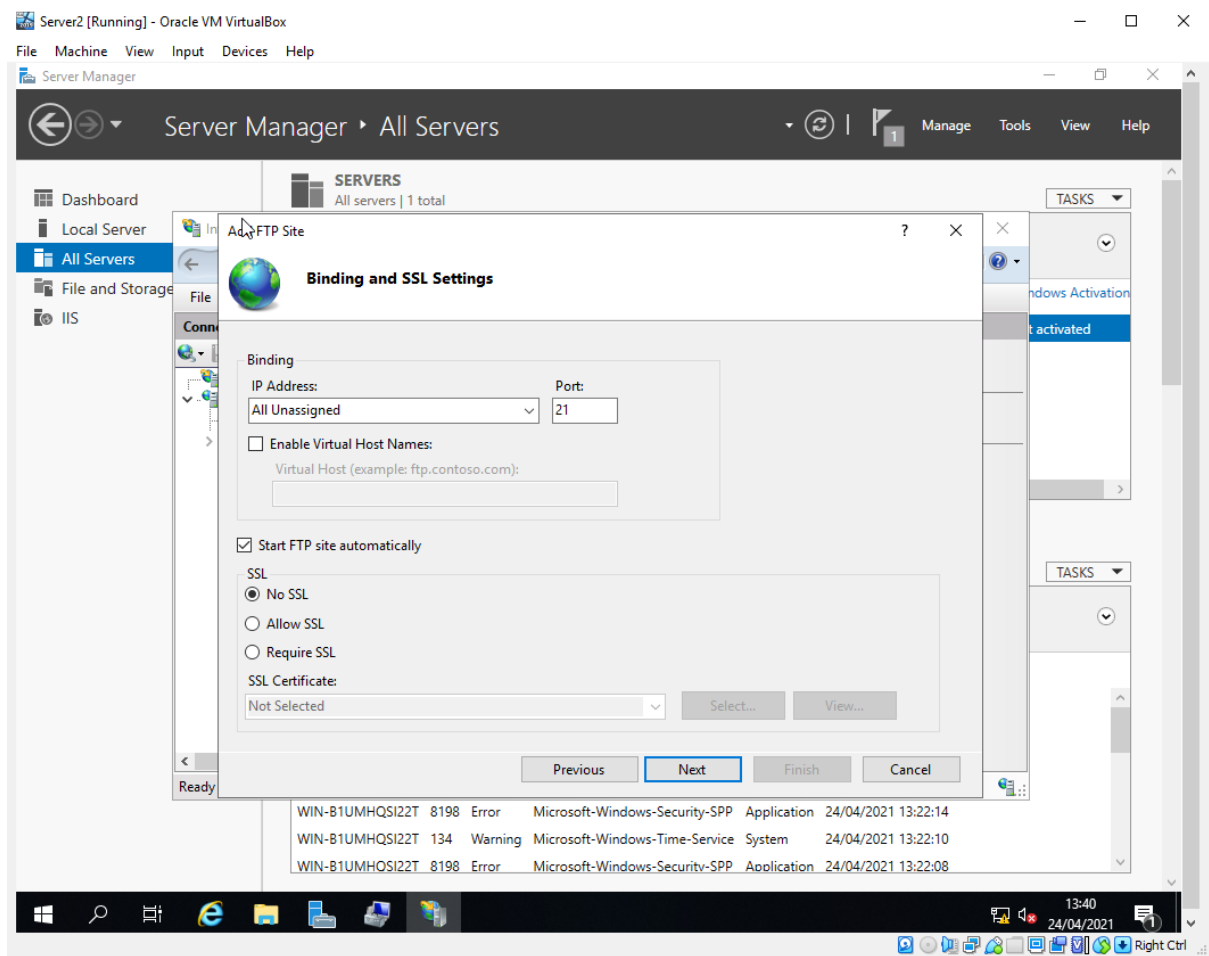


Figure 11 basic authentication configured for FTP site

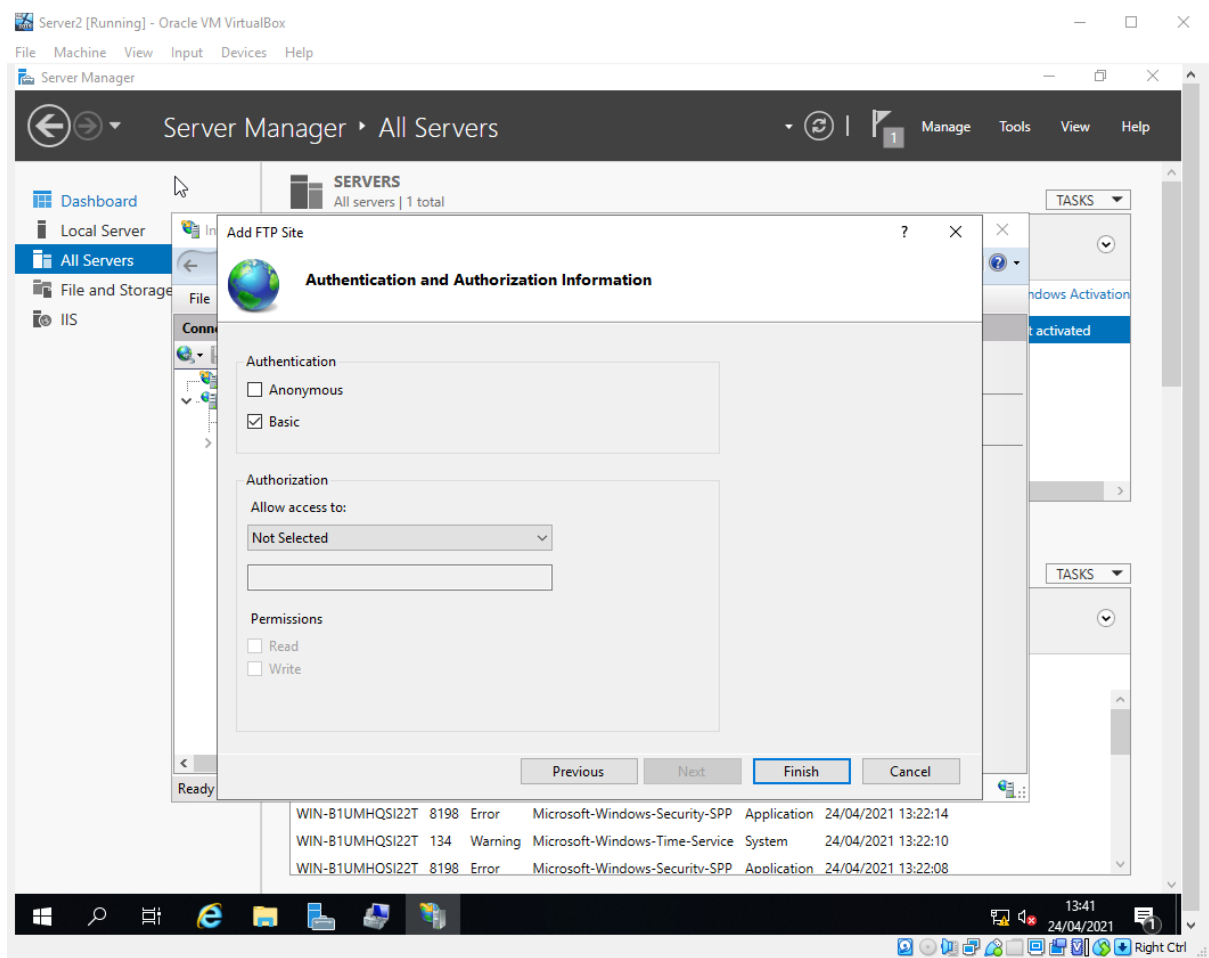


Figure 12 User granted FPT permissions

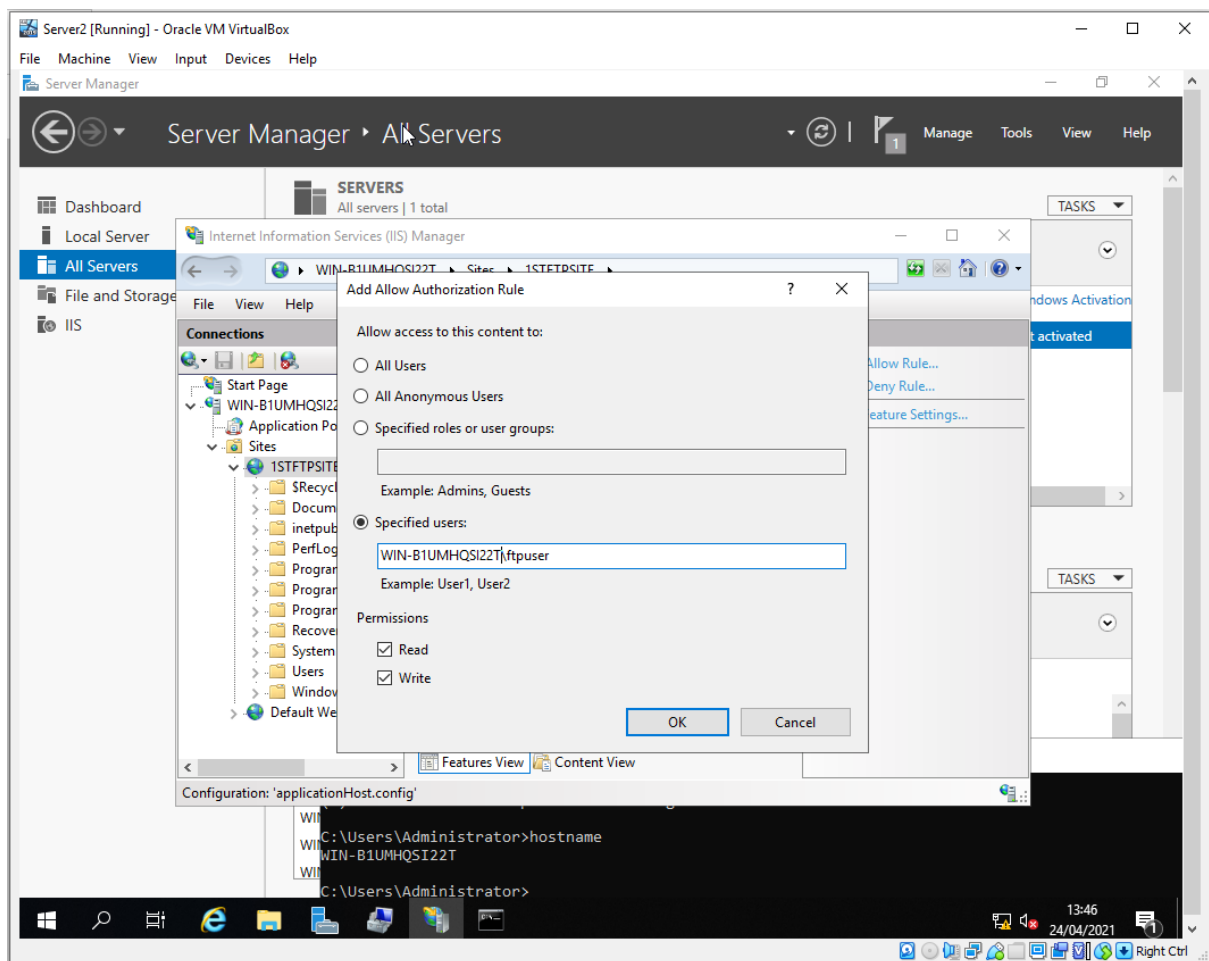


Figure 13 FTP banner created.

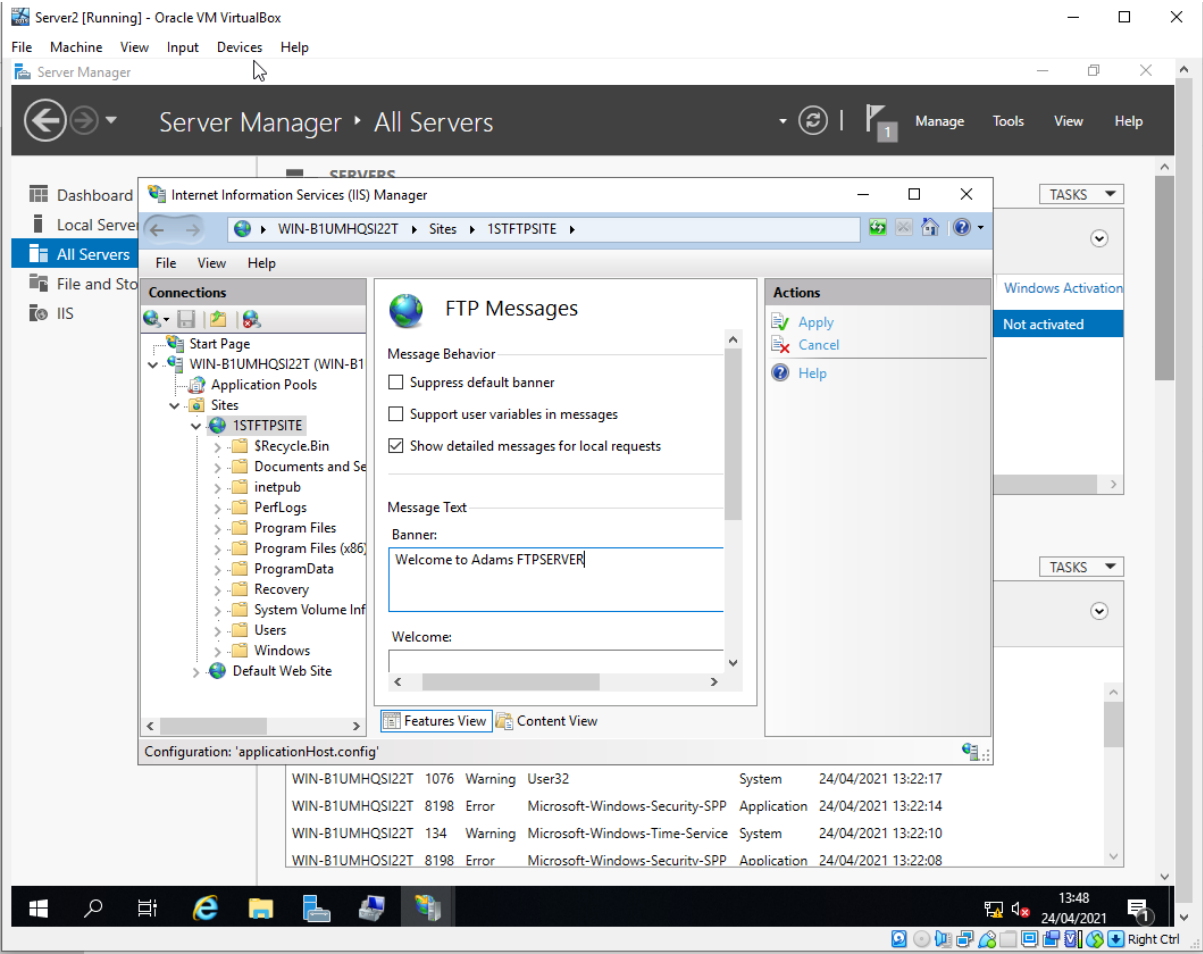


Figure 14ftproot folder permissions granted to FTPUSER

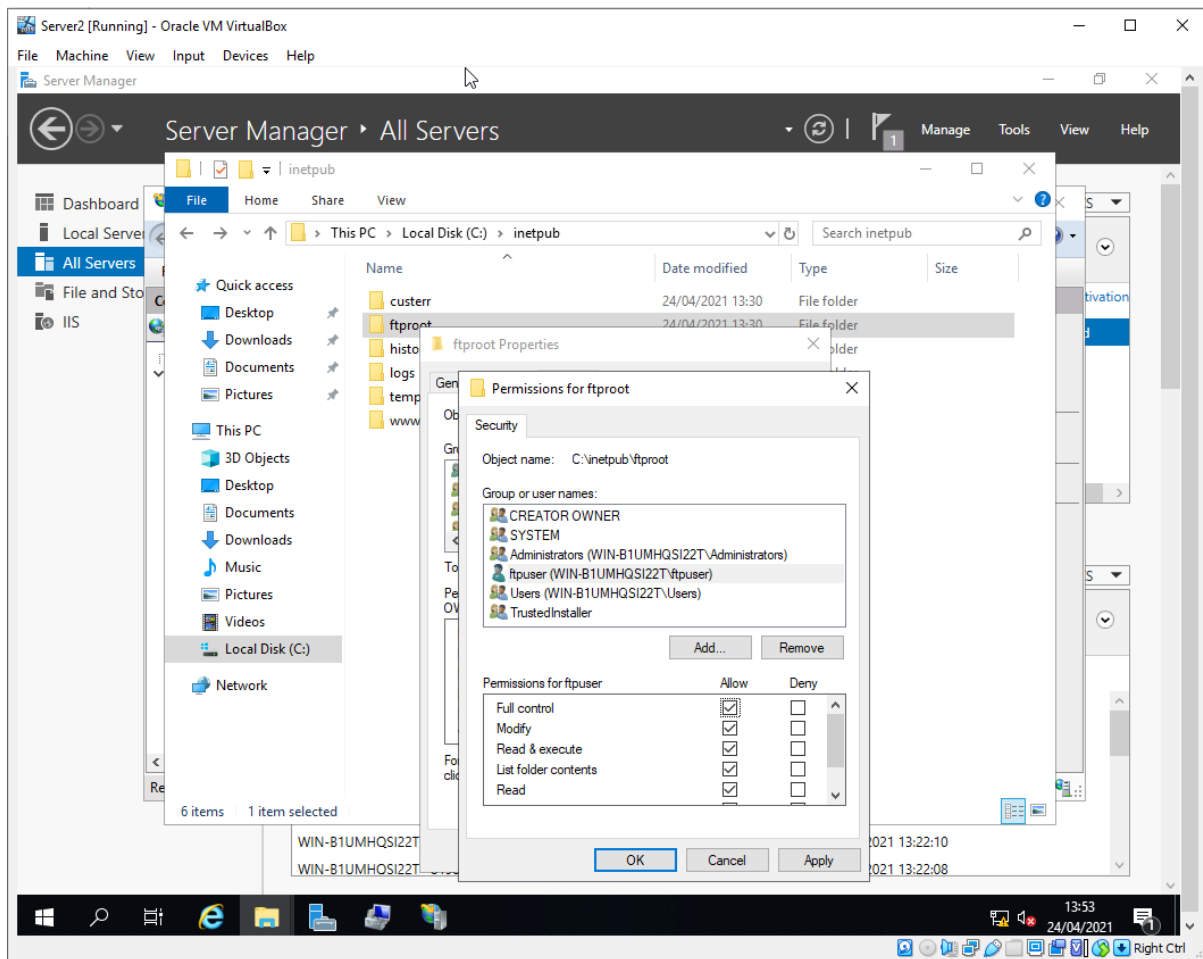


Figure 15 confirmed that the firewall is disabled

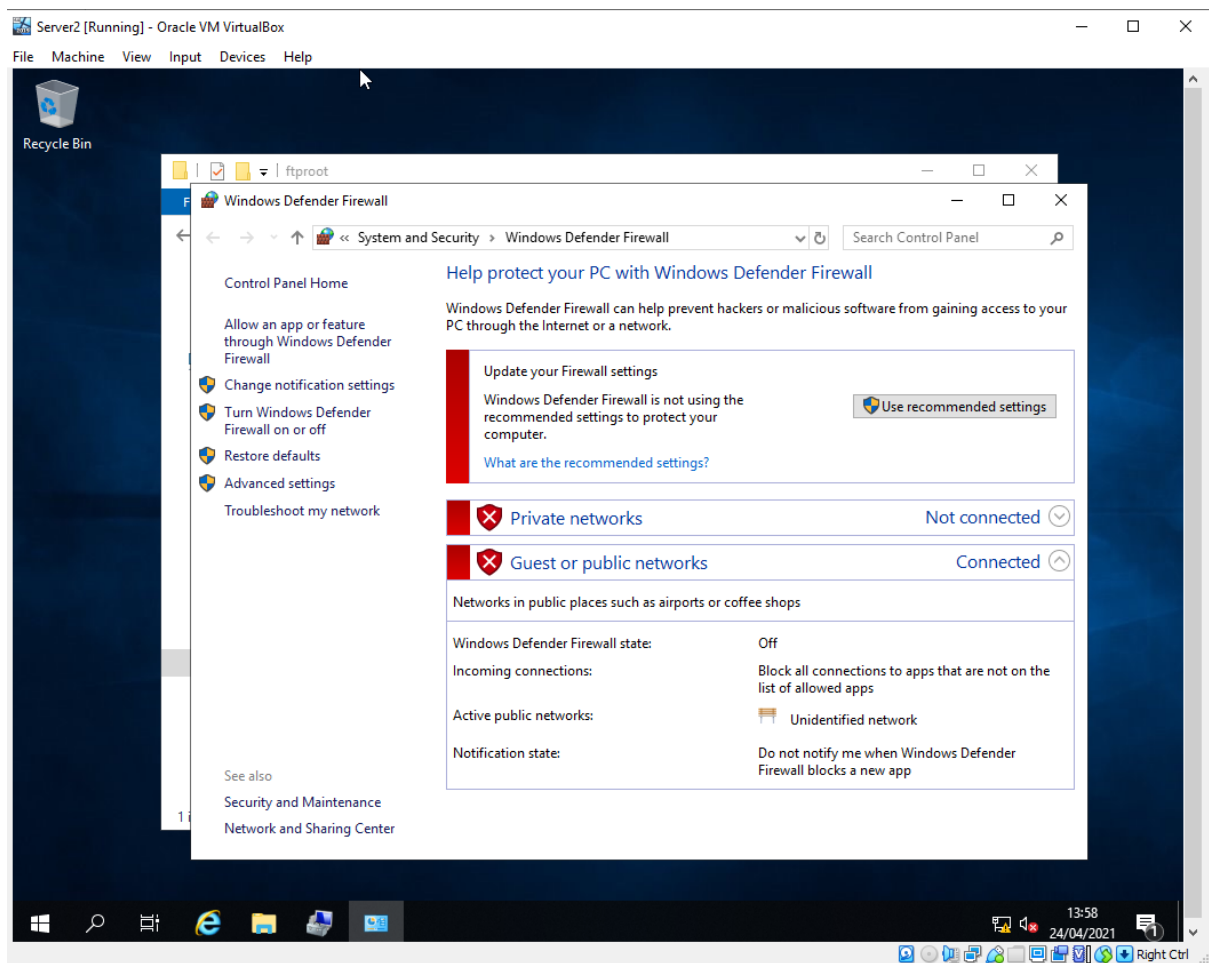


Figure 16 FTP connection established, user logged in, local directory set.

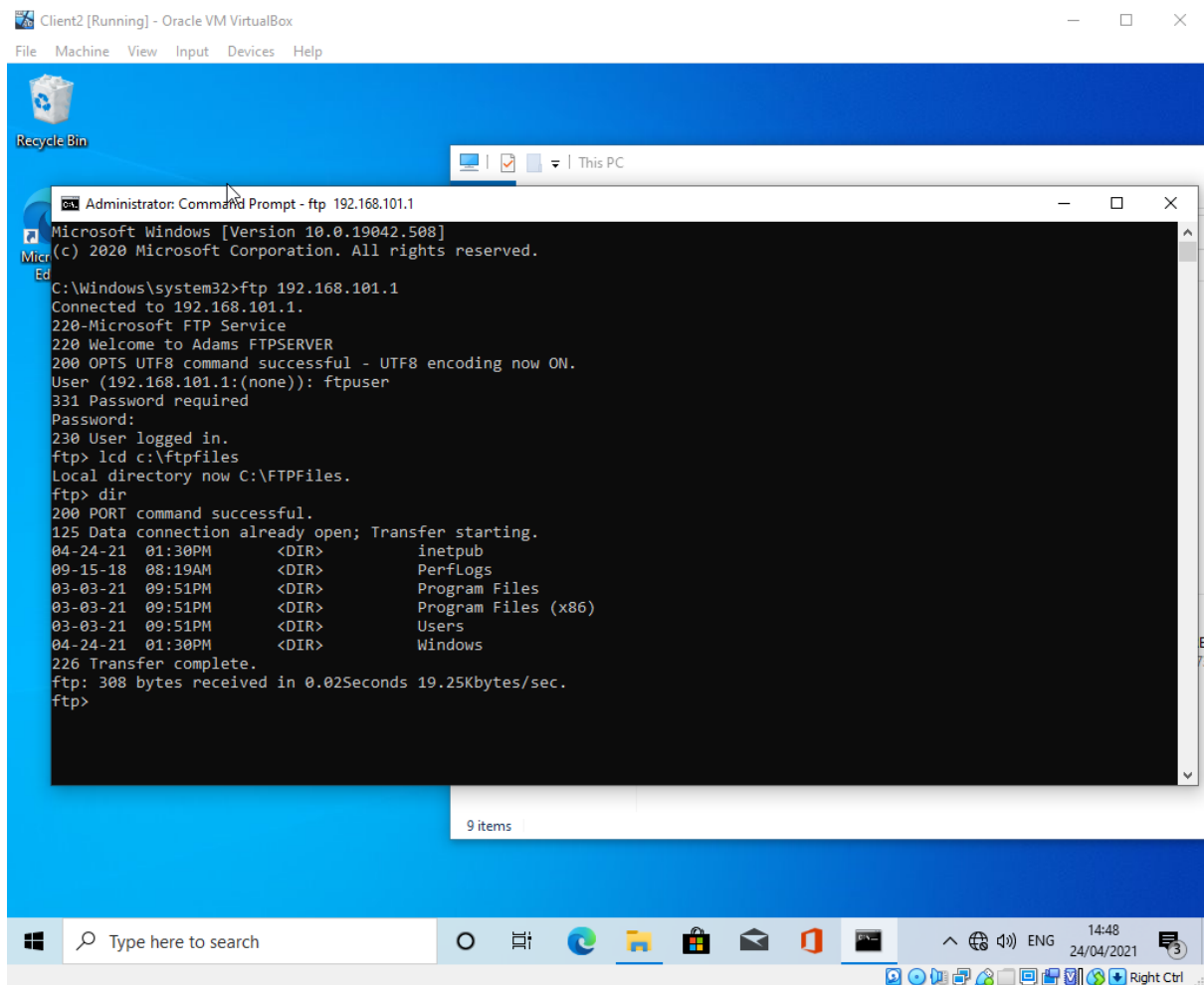
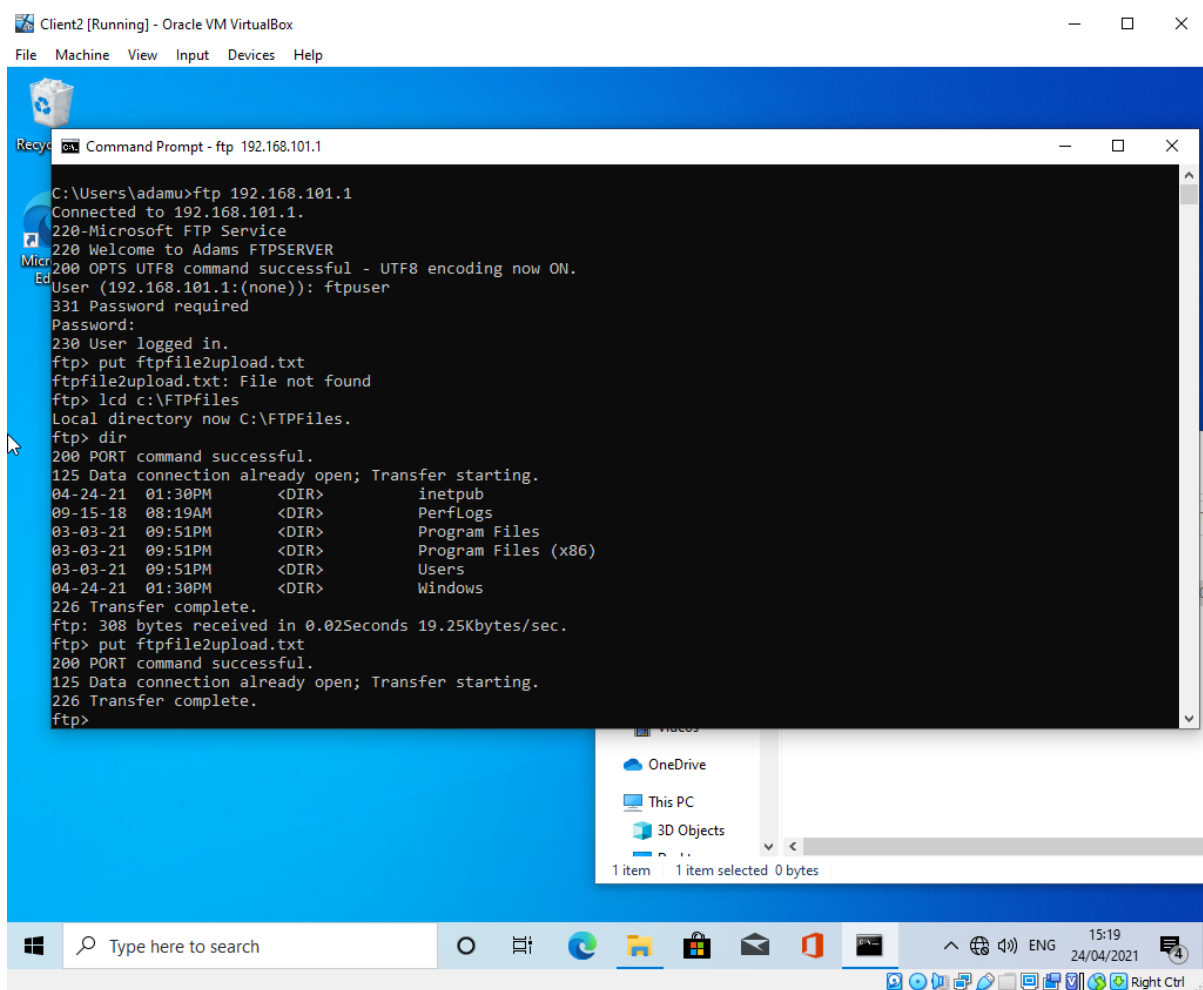


Figure 17 file successfully sent via FTP



Task 3: Installing and configuring the Routing and Remote Access Service

Figure 18 ftp file successfully located on Server2 on root of C following FTP from Client 2

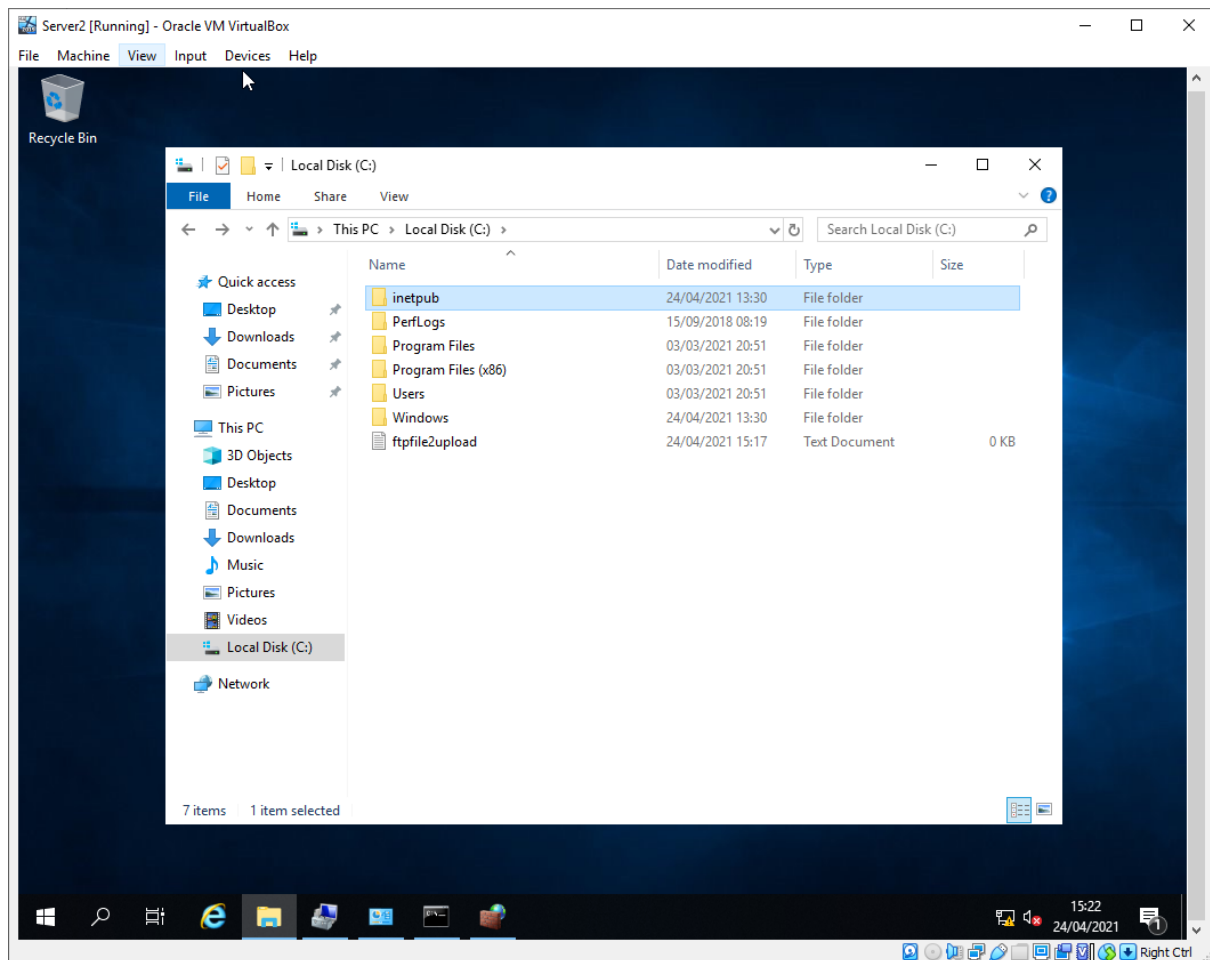


Figure 19 Remote access role selected

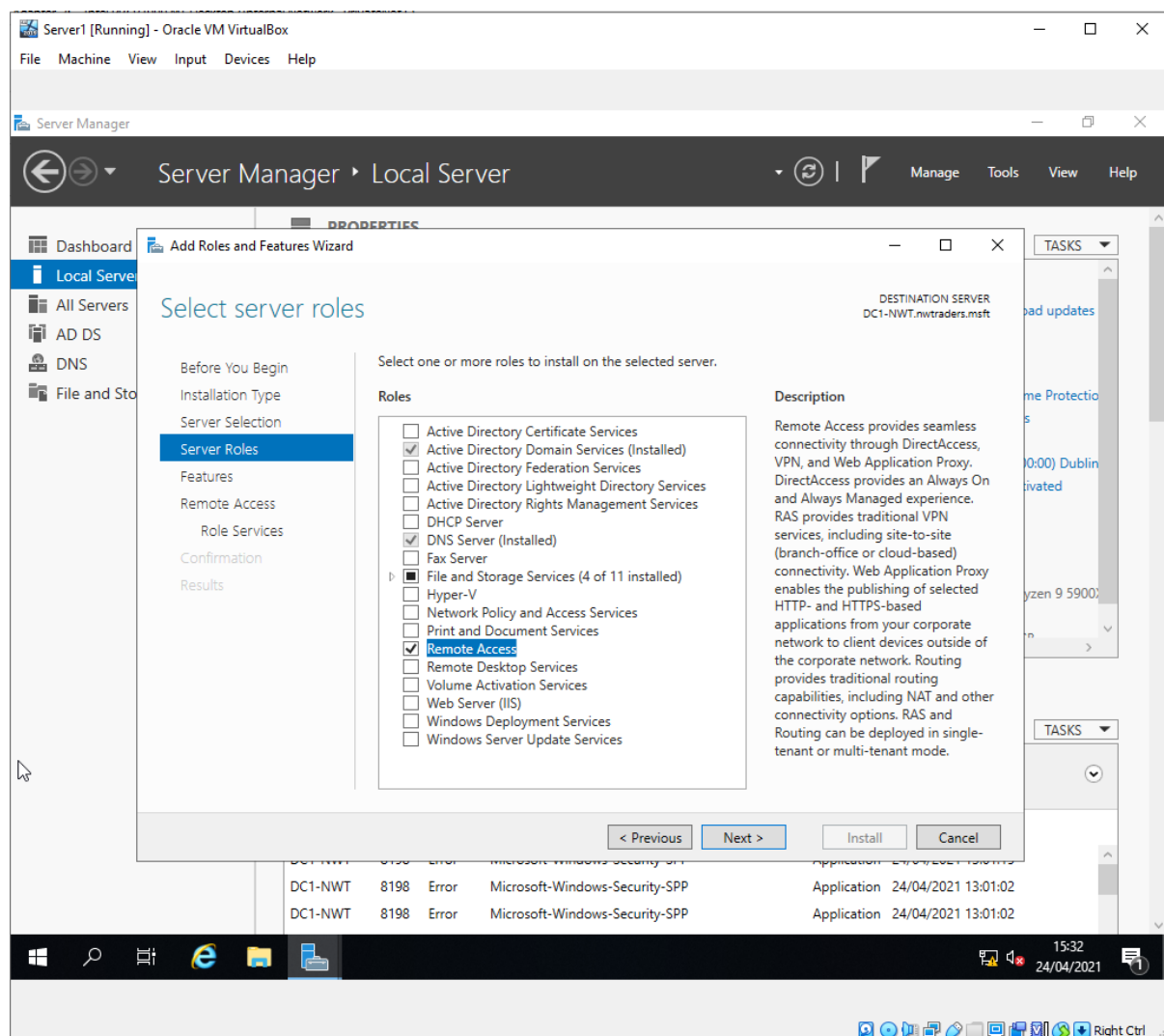


Figure 20 DirectAccess,VPN and routing enabled

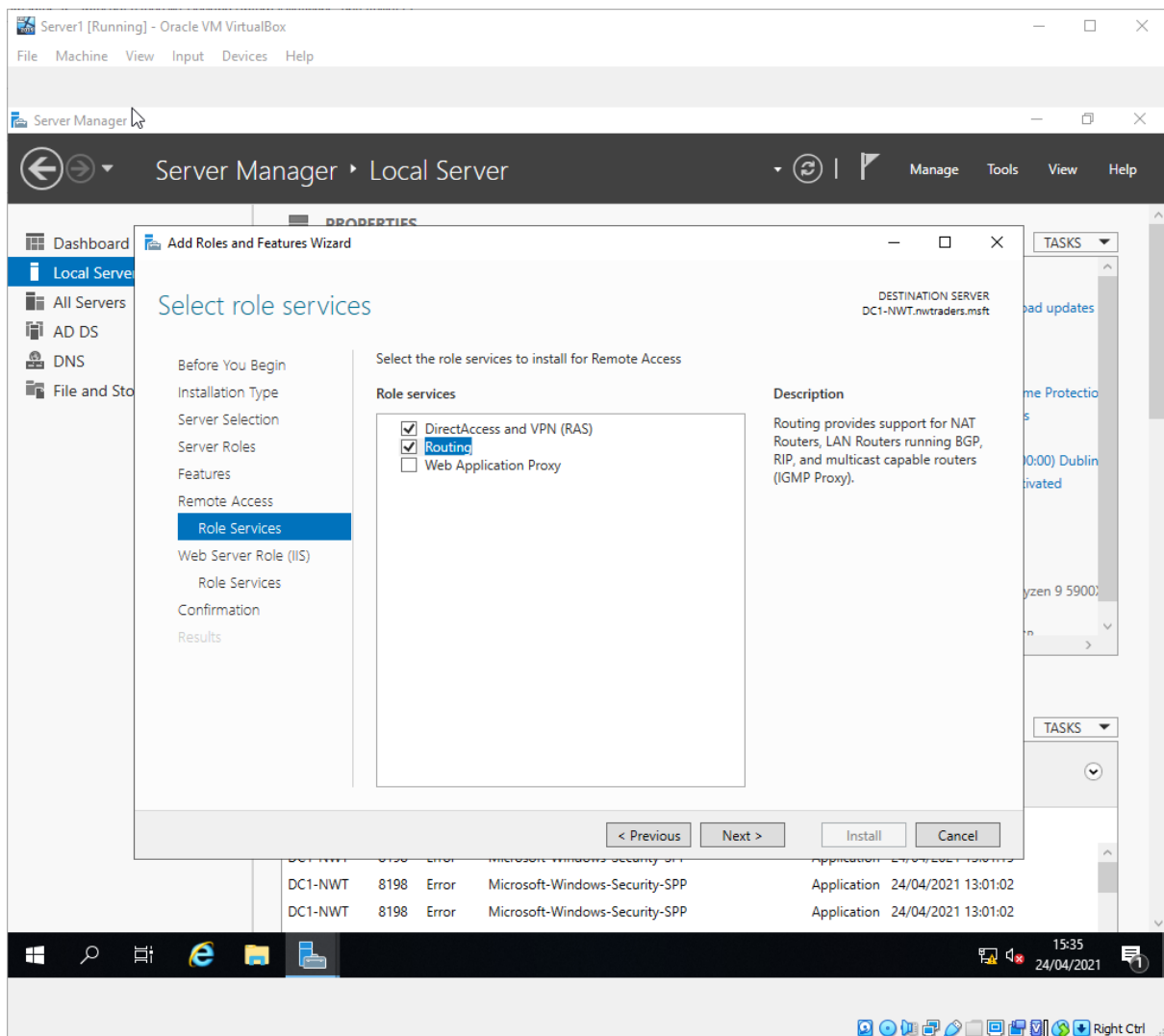


Figure 21 LAN routing enabled

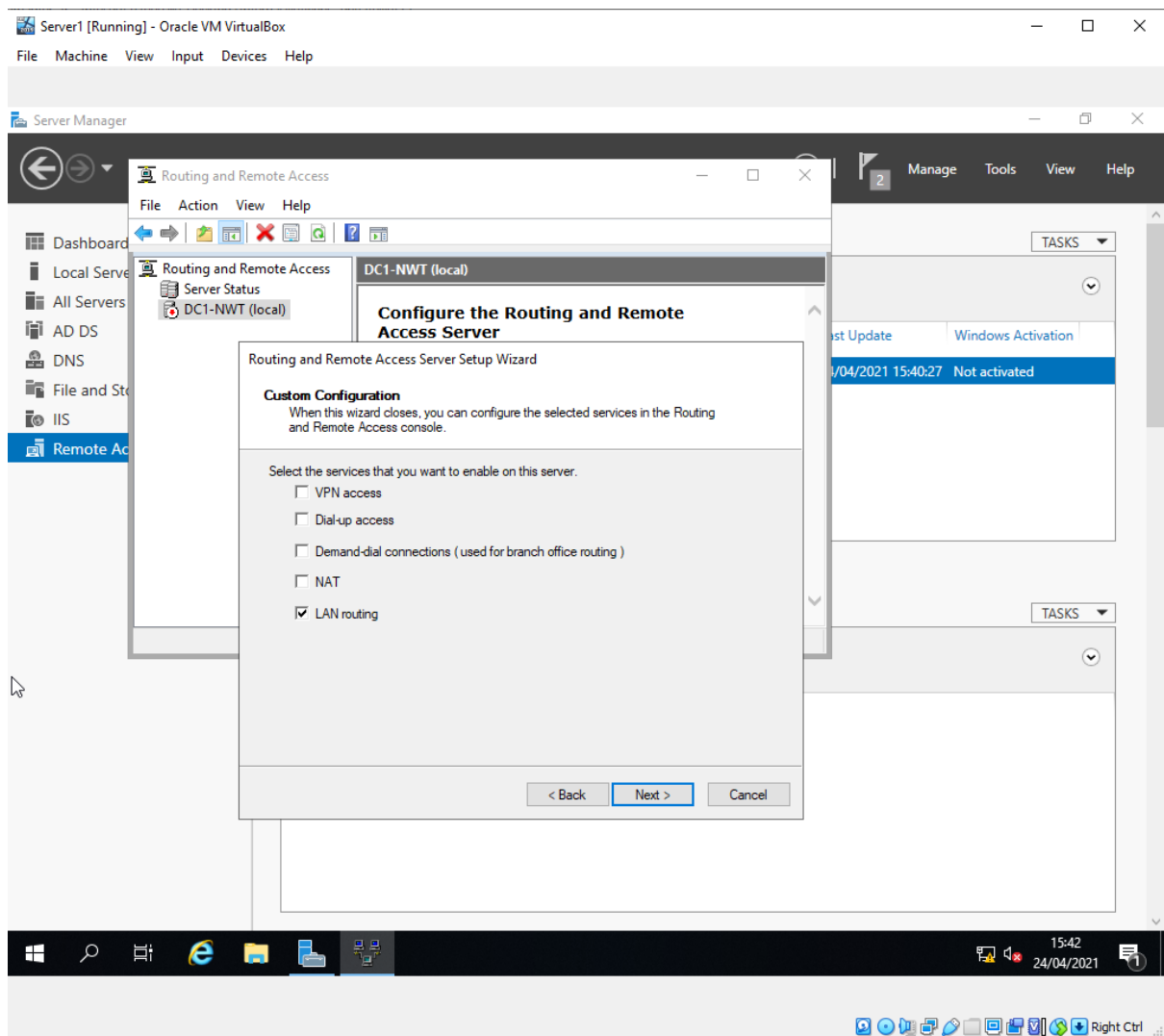


Figure 22 RIP v2 internet protocol selected

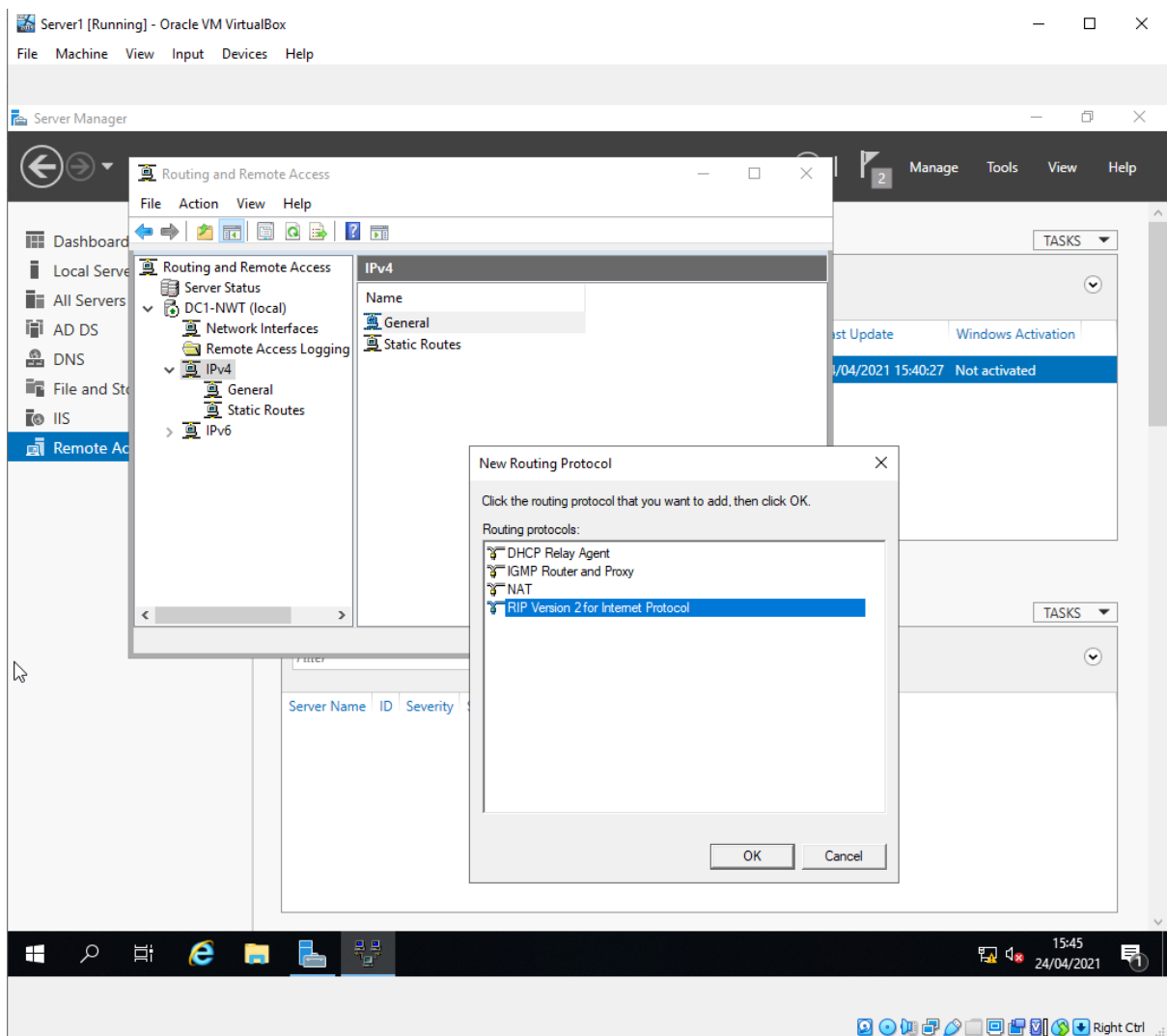


Figure 23 including the privatenet and publicnet interfaces for routing protocol to run on

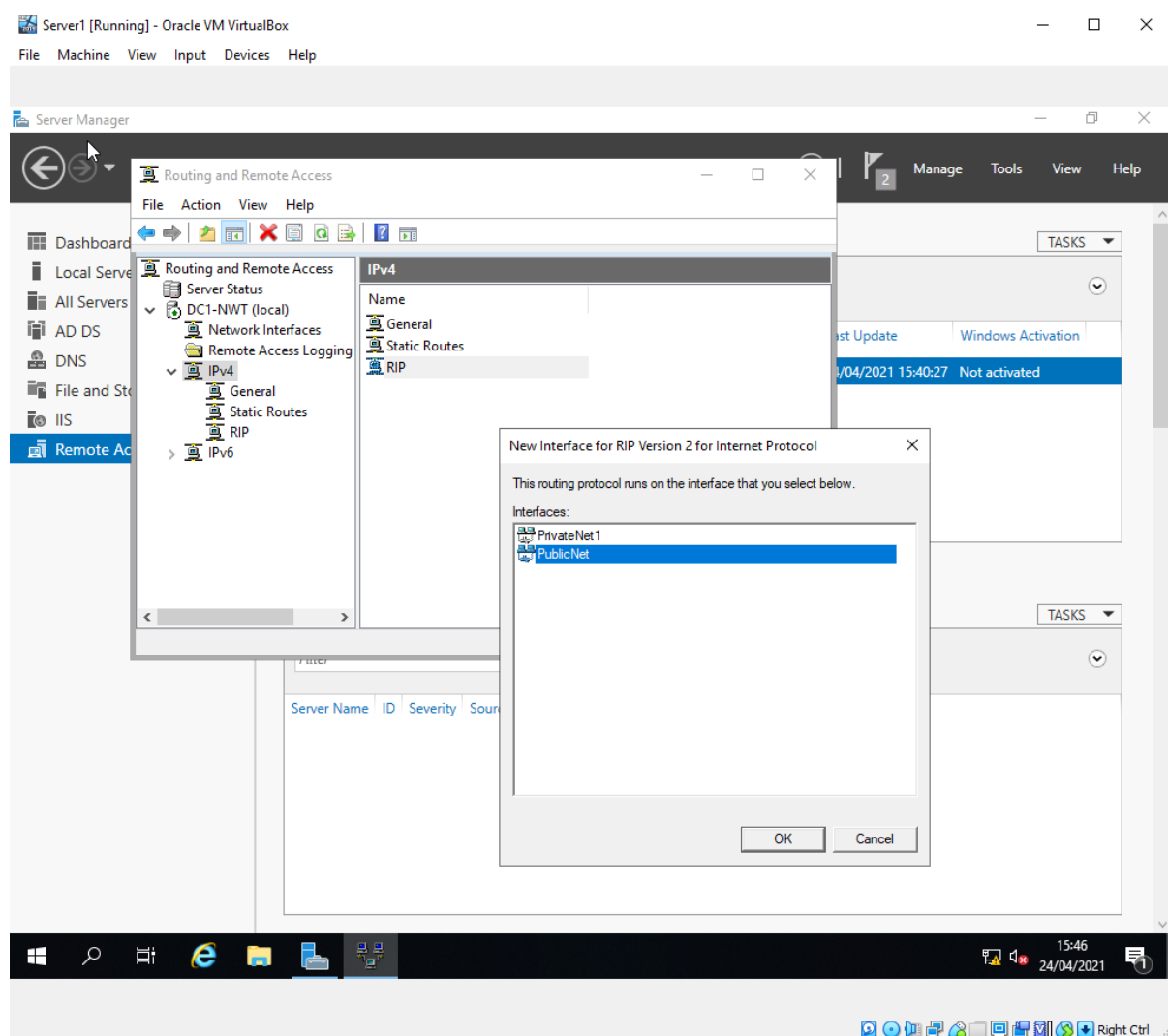


Figure 24 Server 2 configured

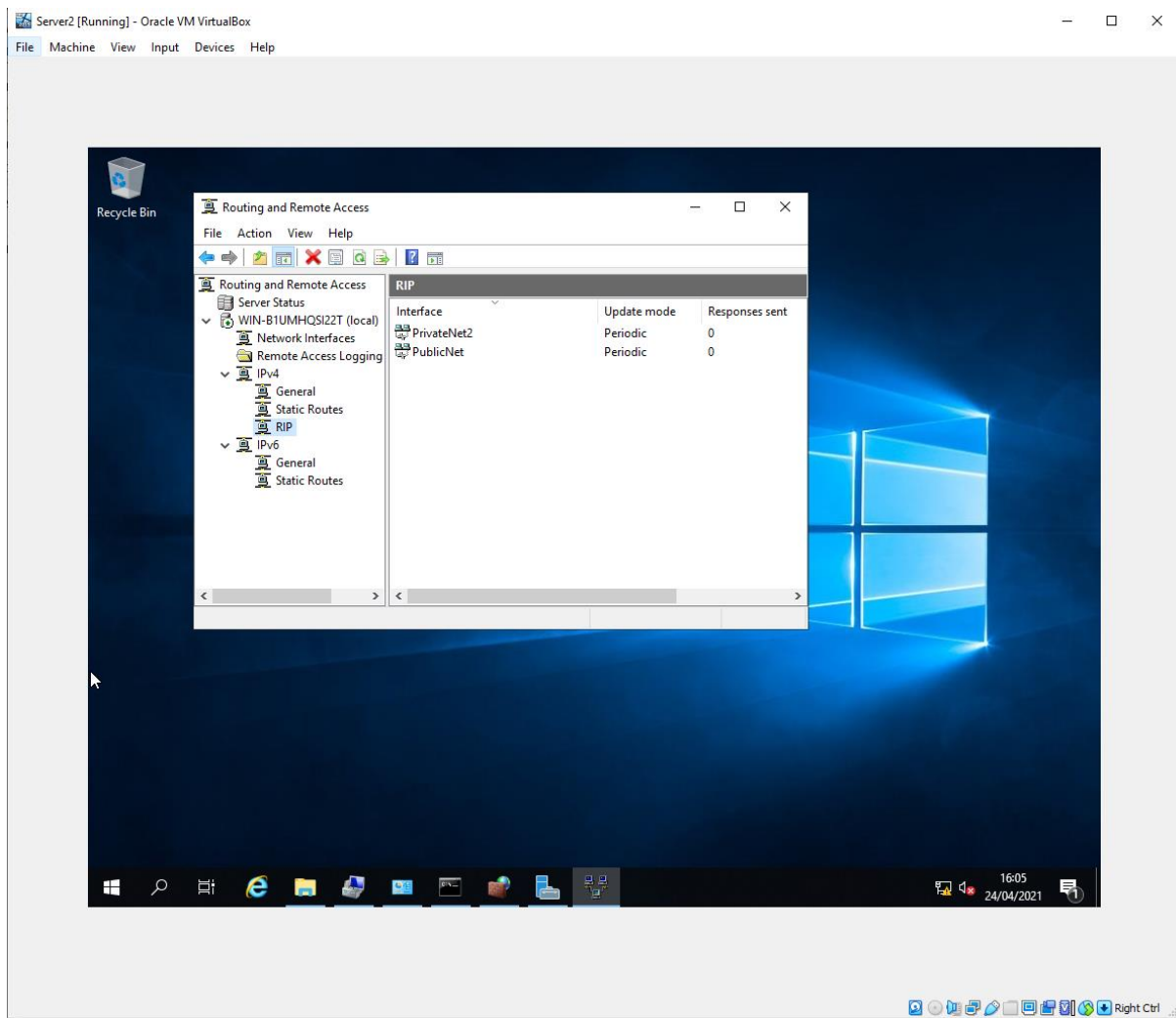


Figure 25 successfully able to ping the “publicnet” ip on server 2 from server 1

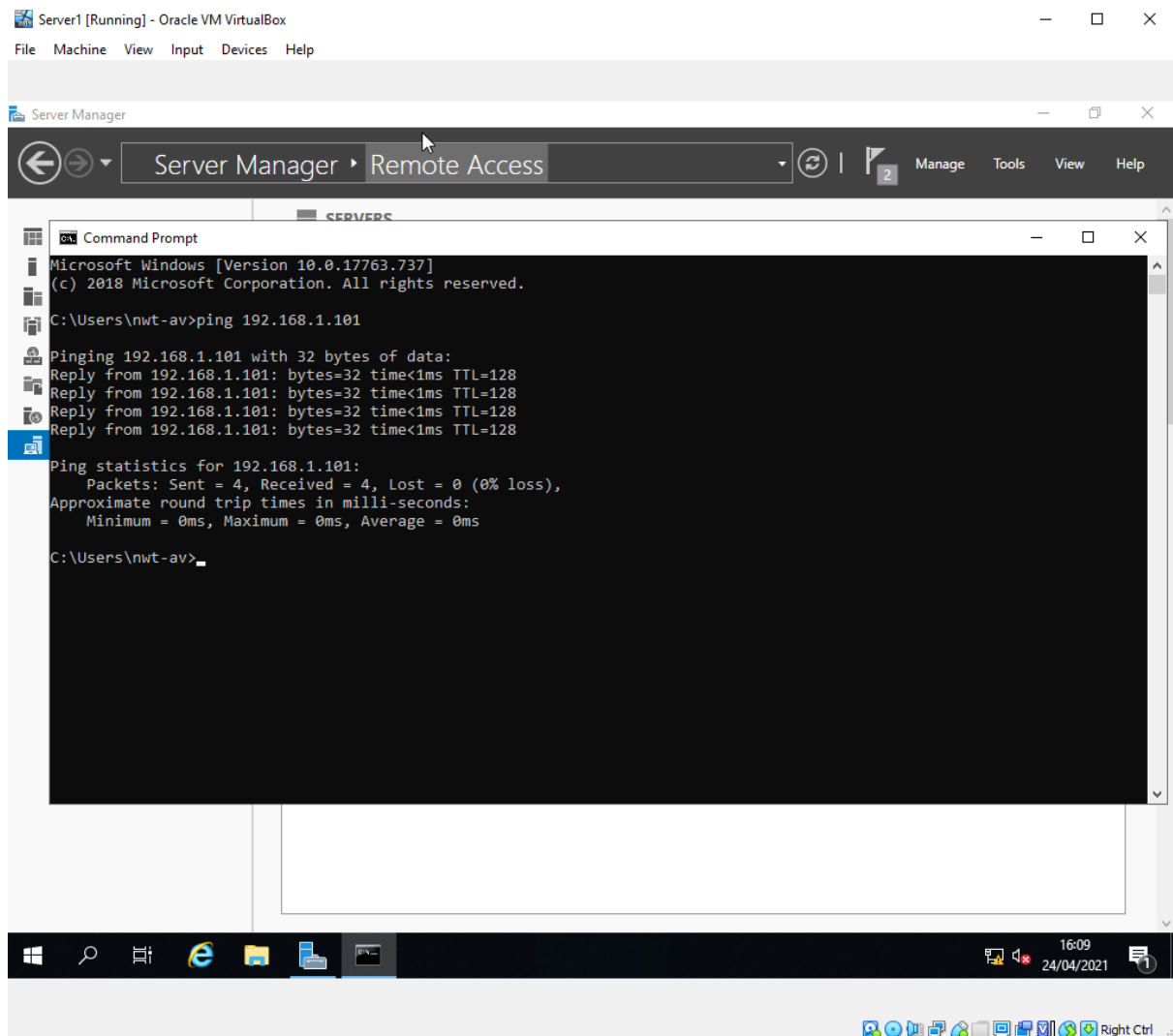
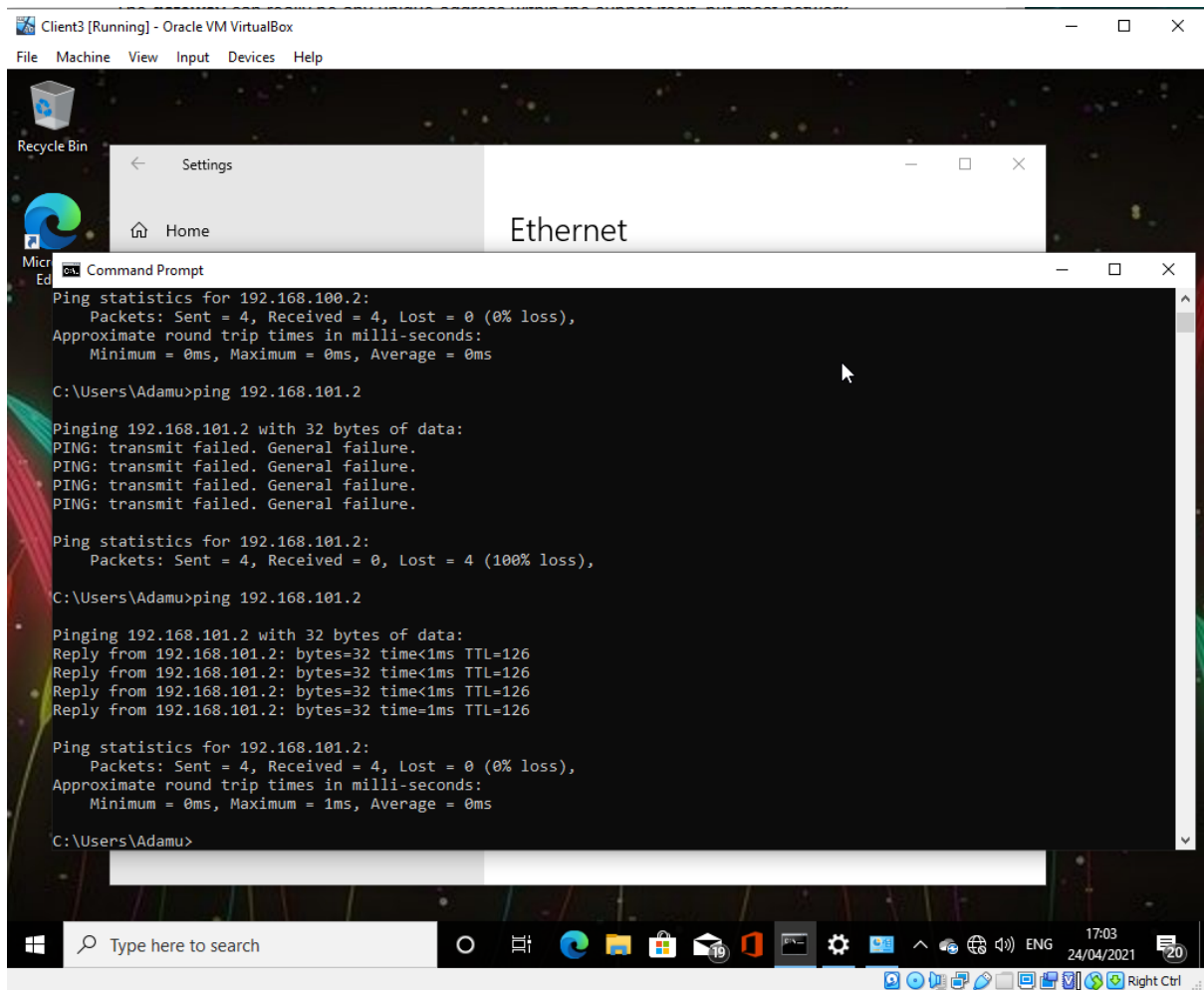


Figure 26 Successful ping attempt following an unsuccessful attempted. Needed to update default gateway on both clients to allow the machines to talk.



IP Packet Filtering

Filter 1: Stopping 'anyone' in PrivateNet 1 from Pinging the Router Firewall Service.

Figure 27 IP Filter added for address: 192.168.100.1 using ICMP protocol

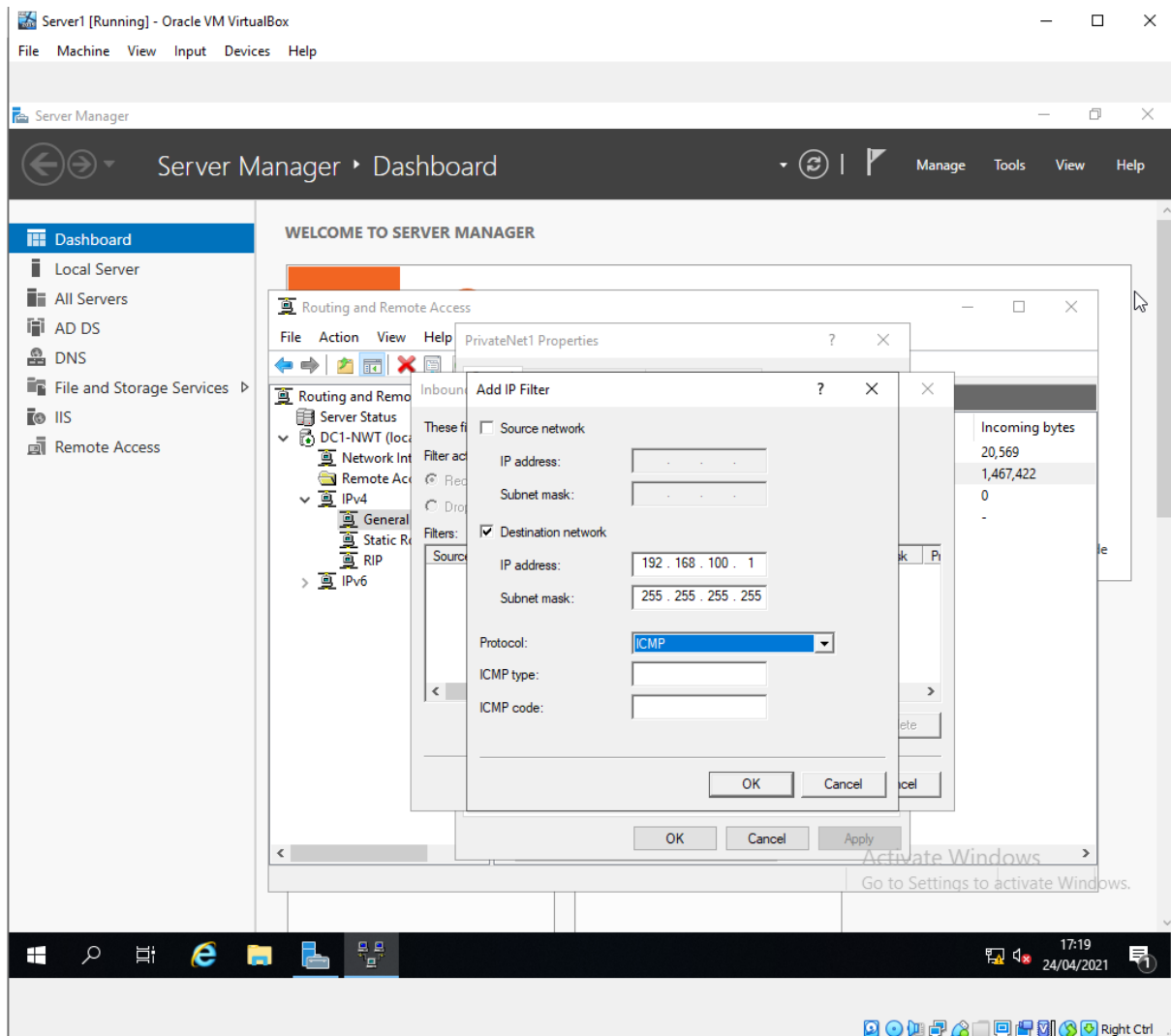


Figure 28 Configured to receive all packets apart from those from on 192.168.100.1

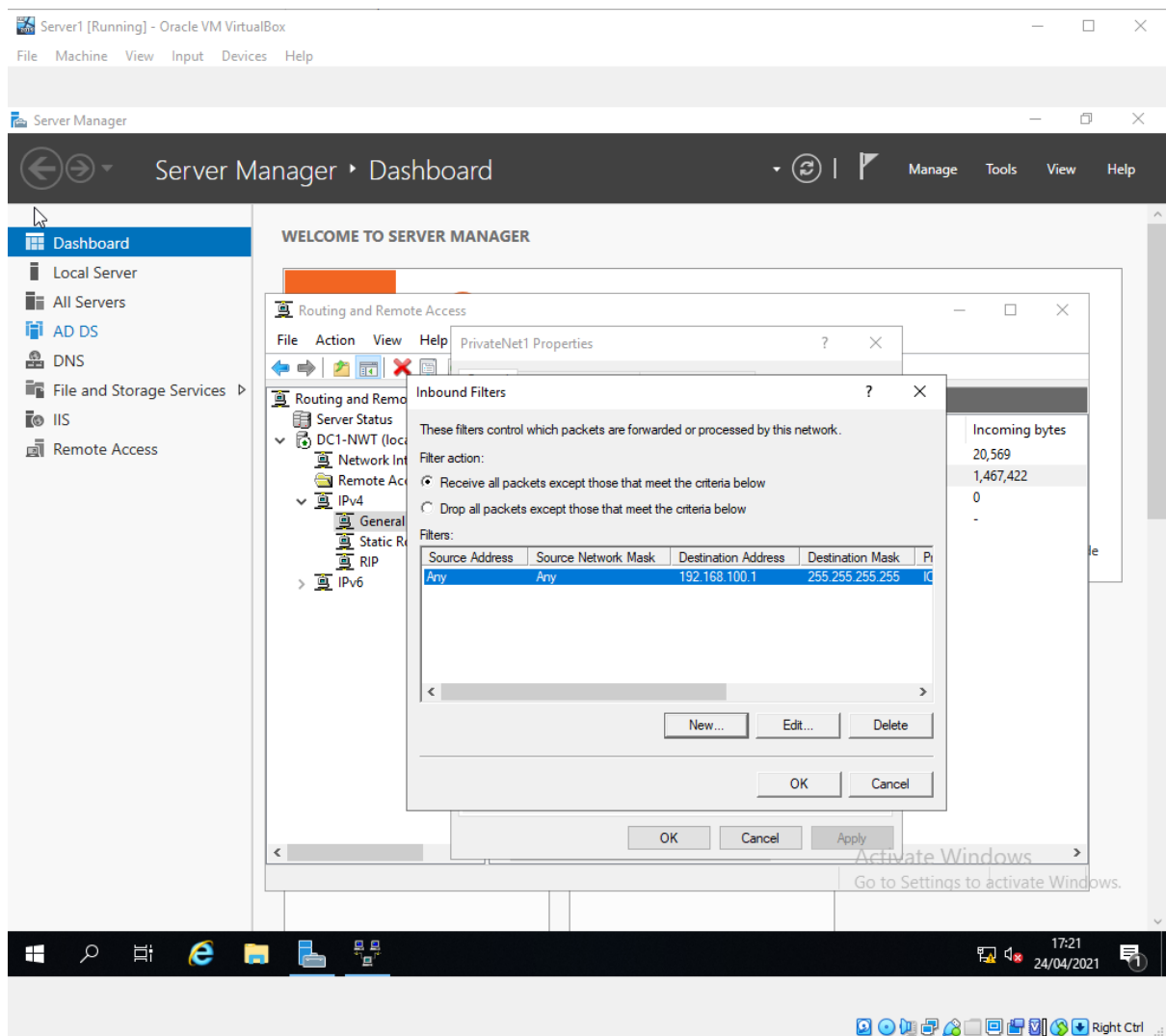
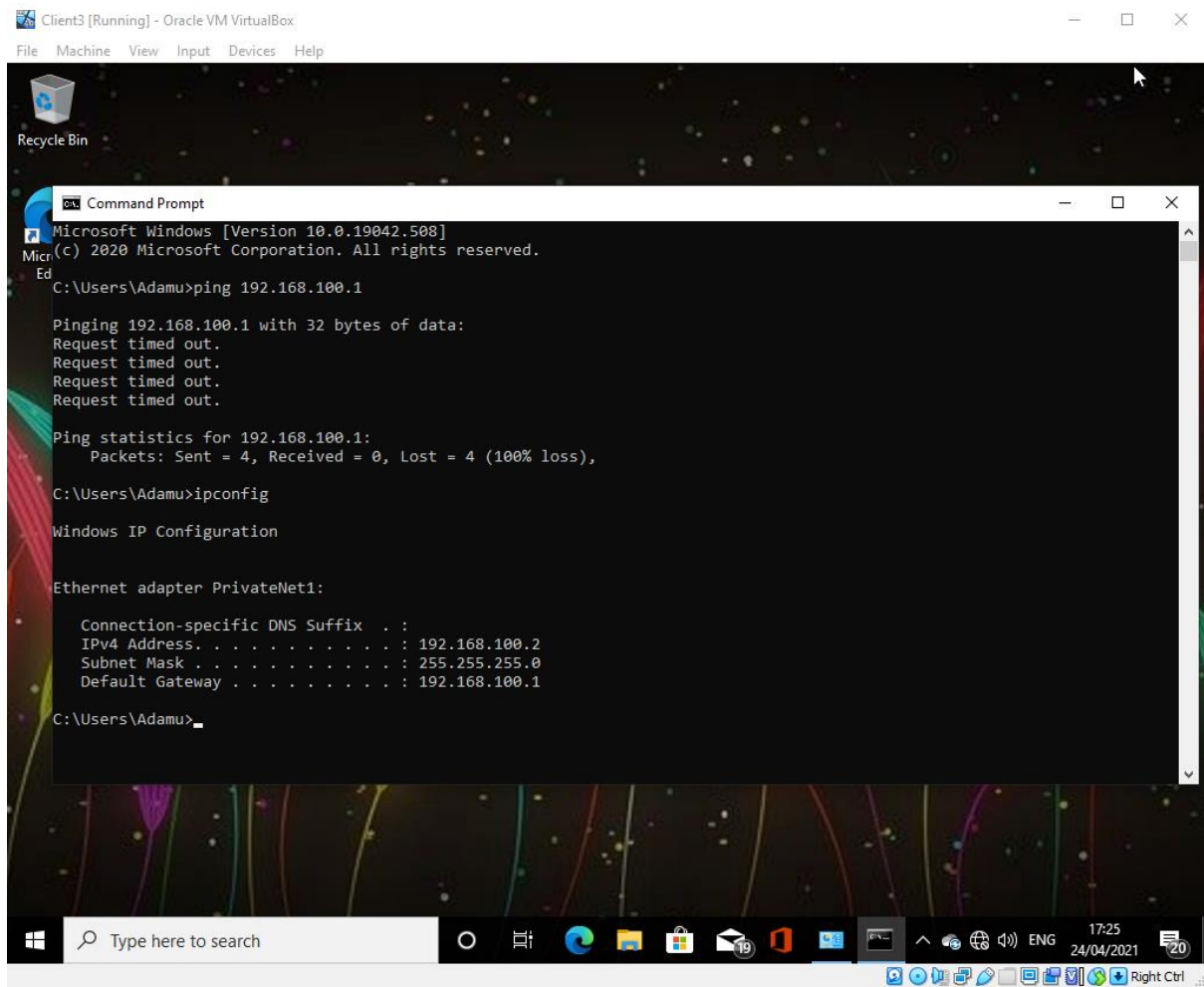


Figure 29 ping from Client1 to Server1 is unsuccessful due to the newly filter denying access



```
Client3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Recycle Bin

Command Prompt
Microsoft Windows [Version 10.0.19042.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Adamu>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Adamu>ipconfig

Windows IP Configuration

Ethernet adapter PrivateNet1:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

C:\Users\Adamu>
```

Filter 2: Restrict Access to FTP Service running on Server2 to only hosts in PrivateNet2.

Figure 30 additional filter added on server 1

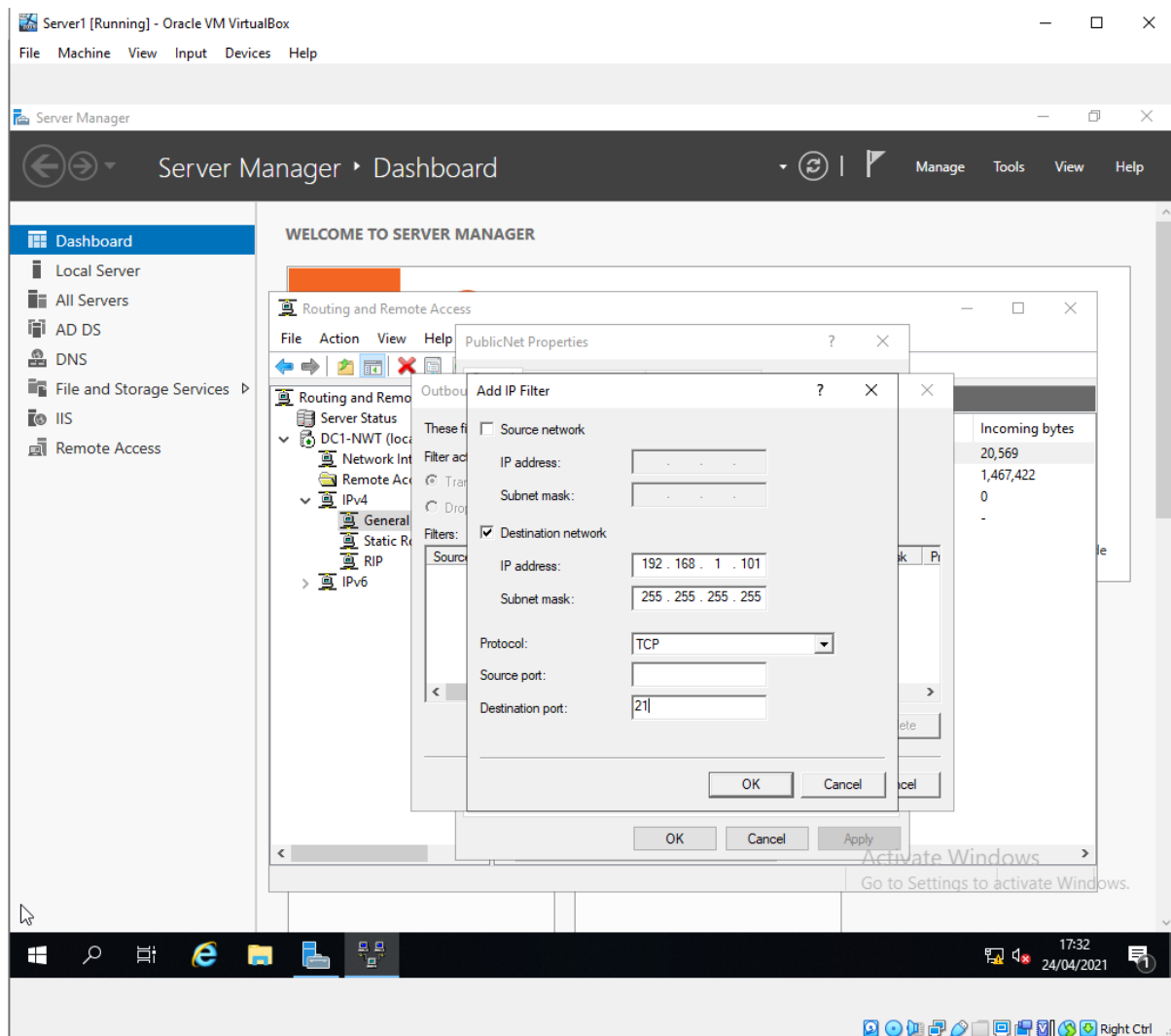


Figure 31 client 1 is still able to access the FTP service on server2

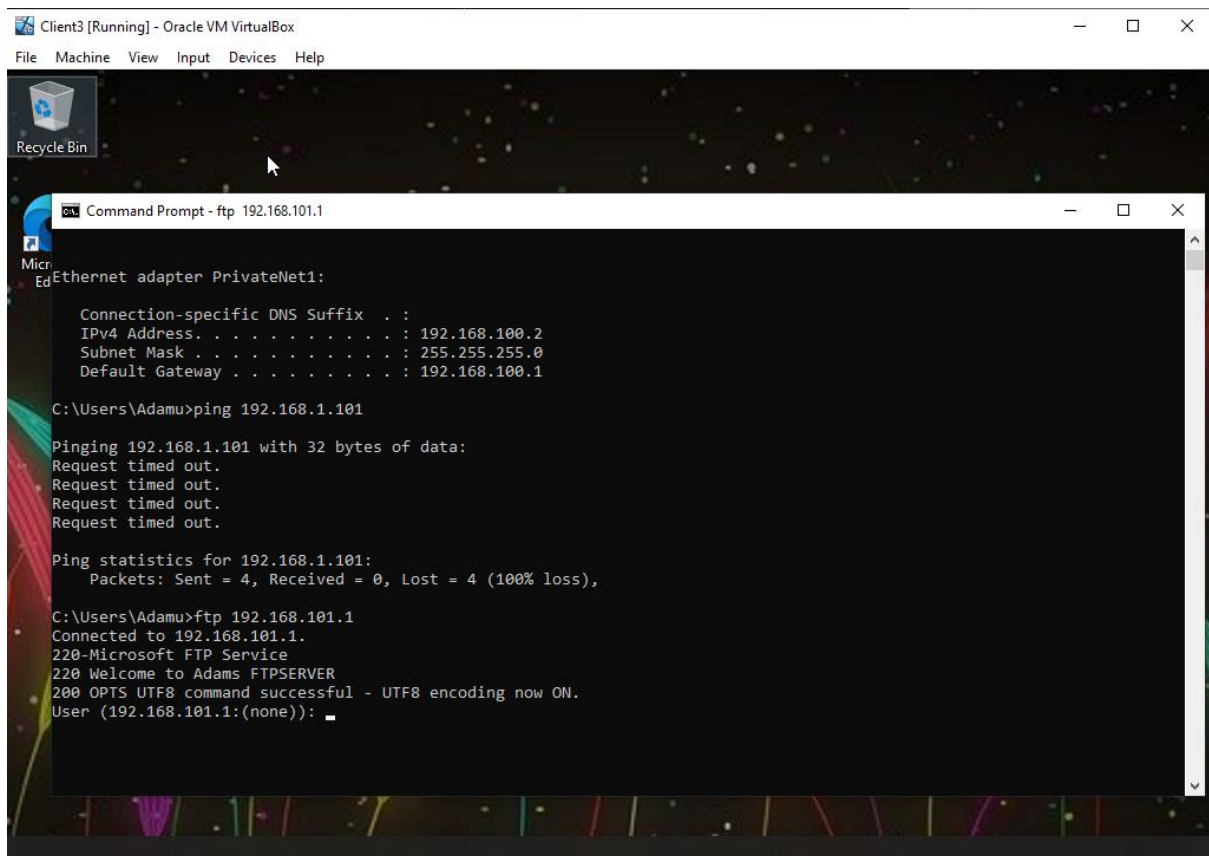


Figure 32 New rule created but focusing on destination port 20

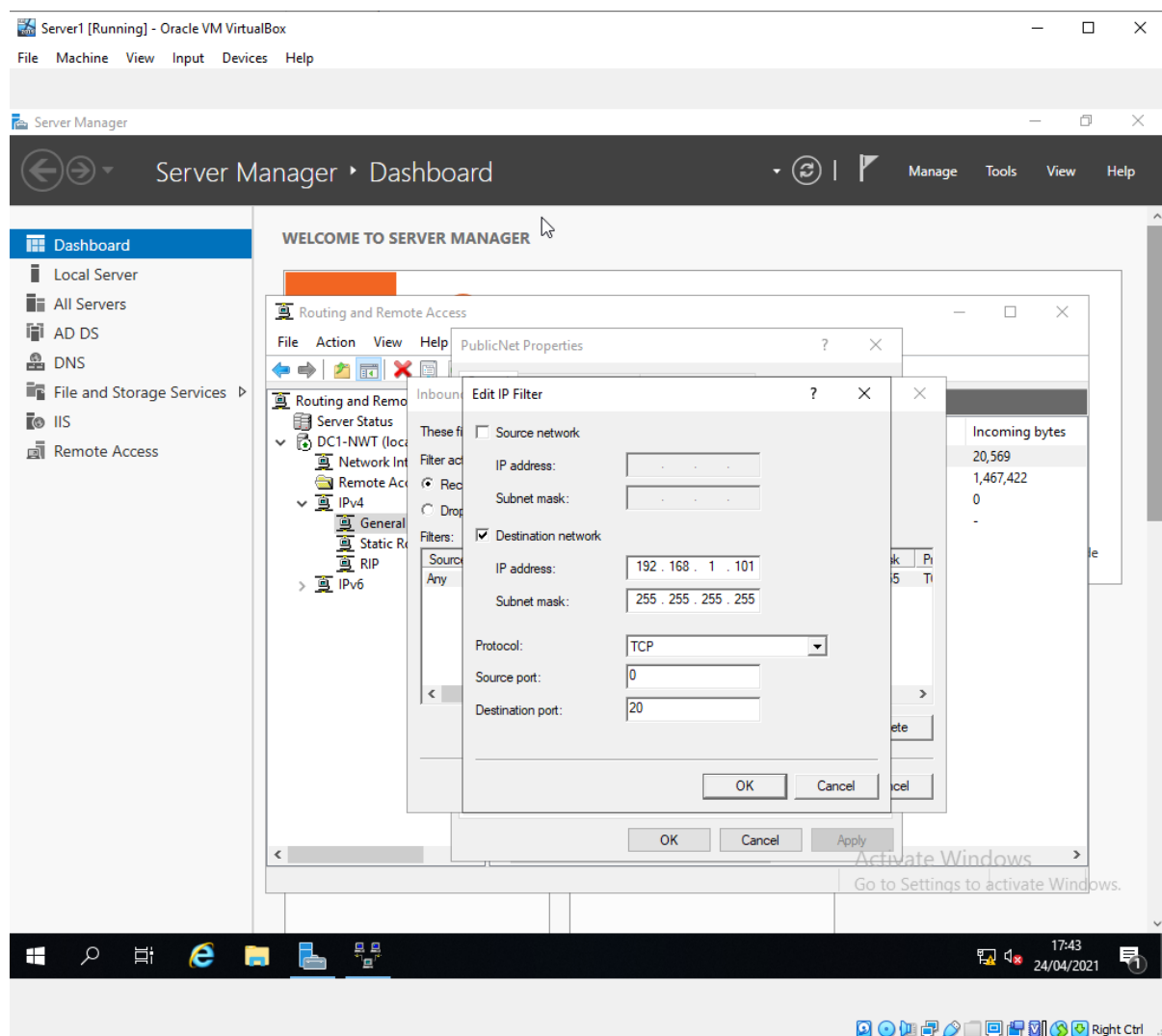


Figure 33 client 3 is still able to talk to the FTP server

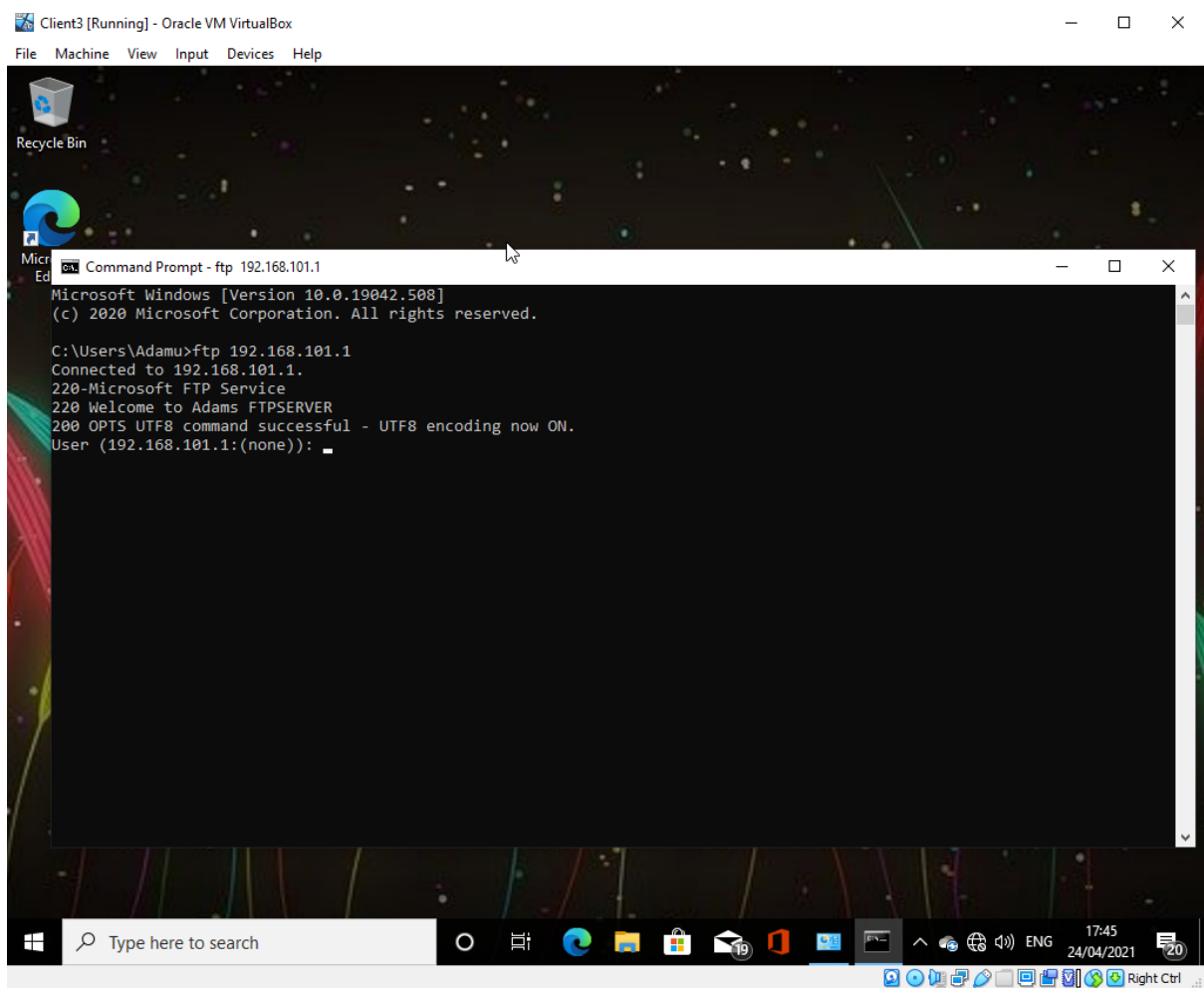


Figure 34 created new rule on server 2 to filter out request from client 1

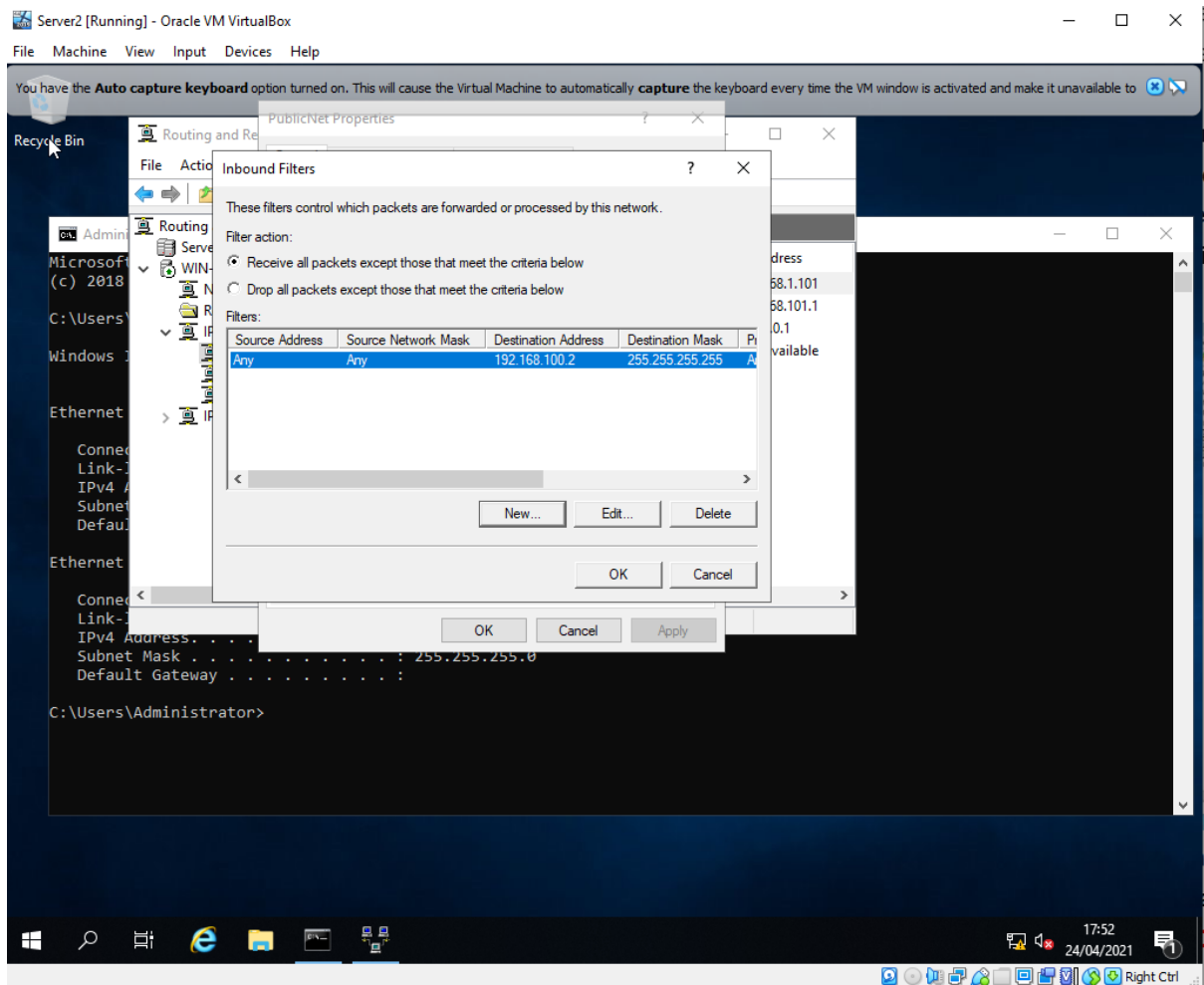
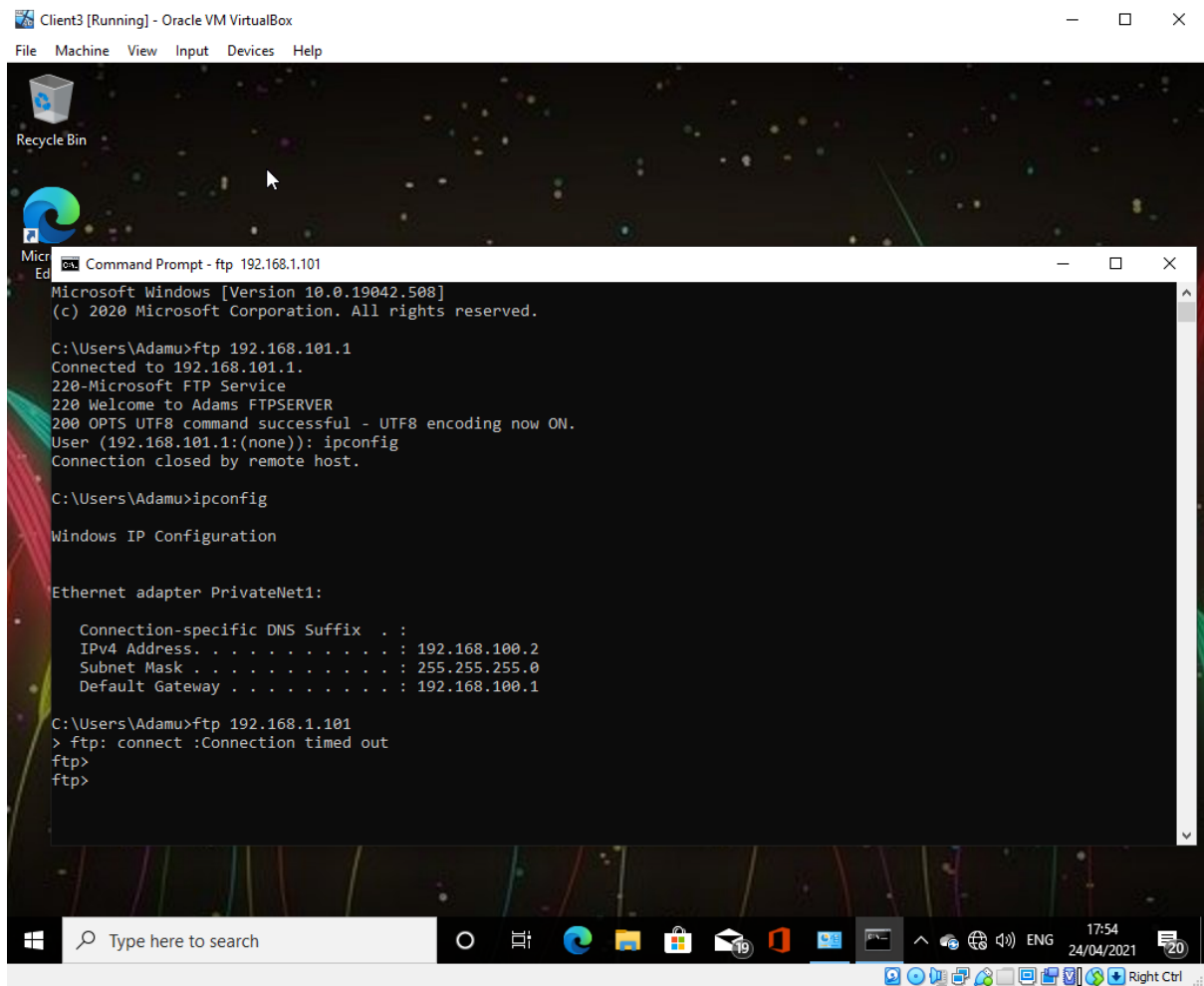


Figure 35 No longer possible to access FTP server from client 1



Filter 3: Only allow specific hosts in PrivateNet1 to access the FTPService running on Server2

Figure 36 Created a new rule for on the FTP “server2” to “Drop all packets except those that meet the criteria below”. This filters out ALL network traffic on the privatenet network apart from request from client 1 as specified below.

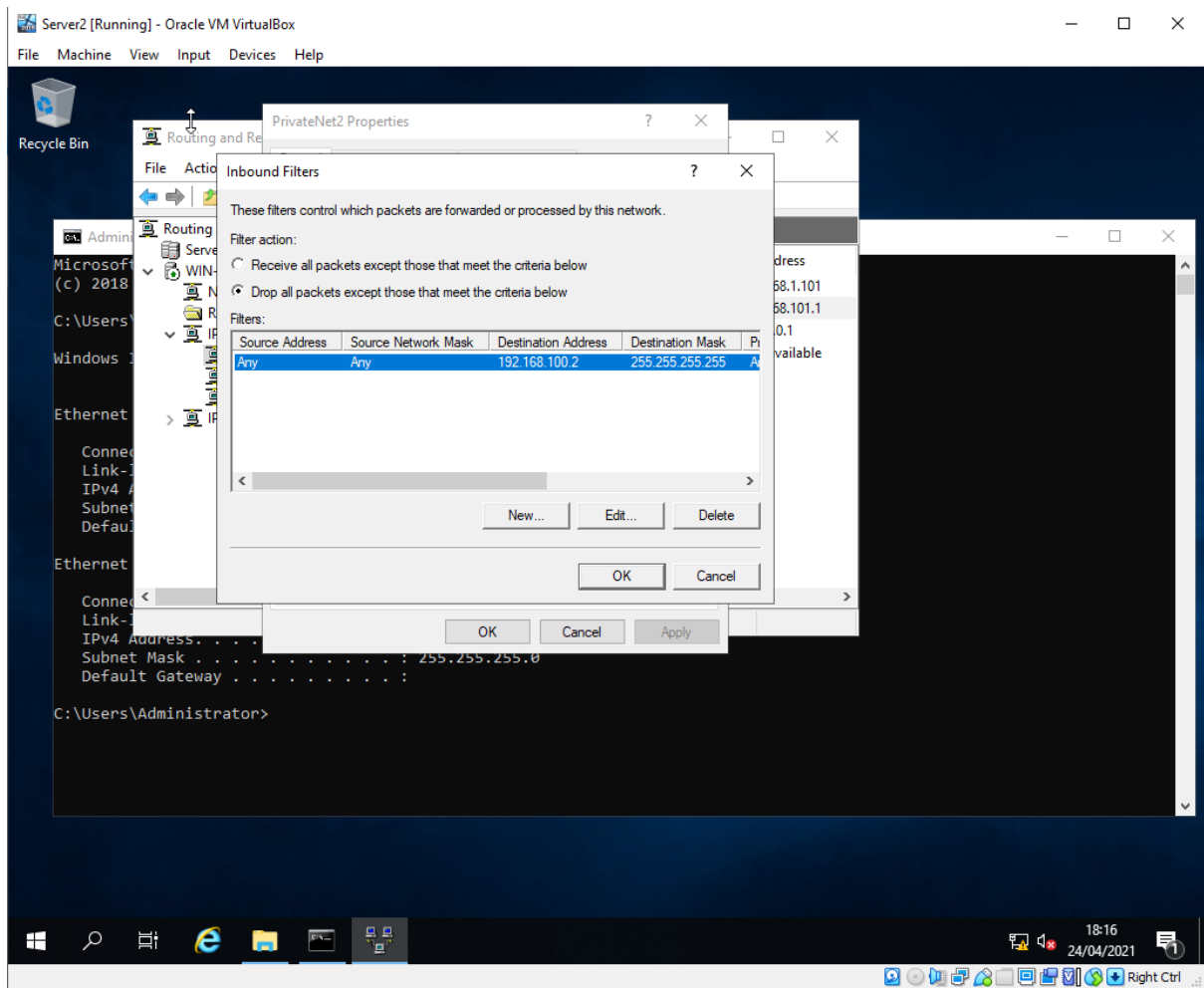


Figure 37 Evidence that client 1 can get through the filter and FTP to server2

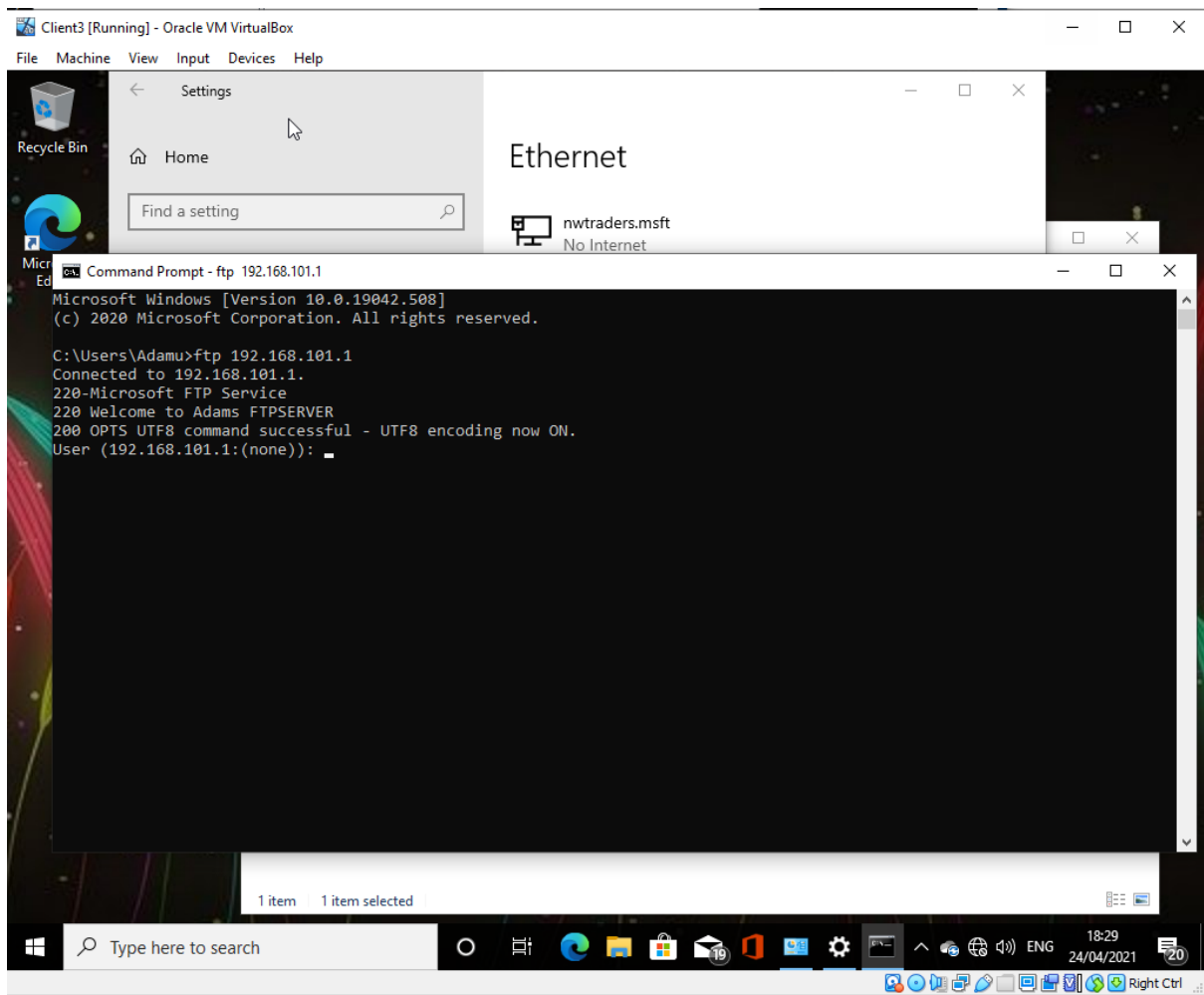
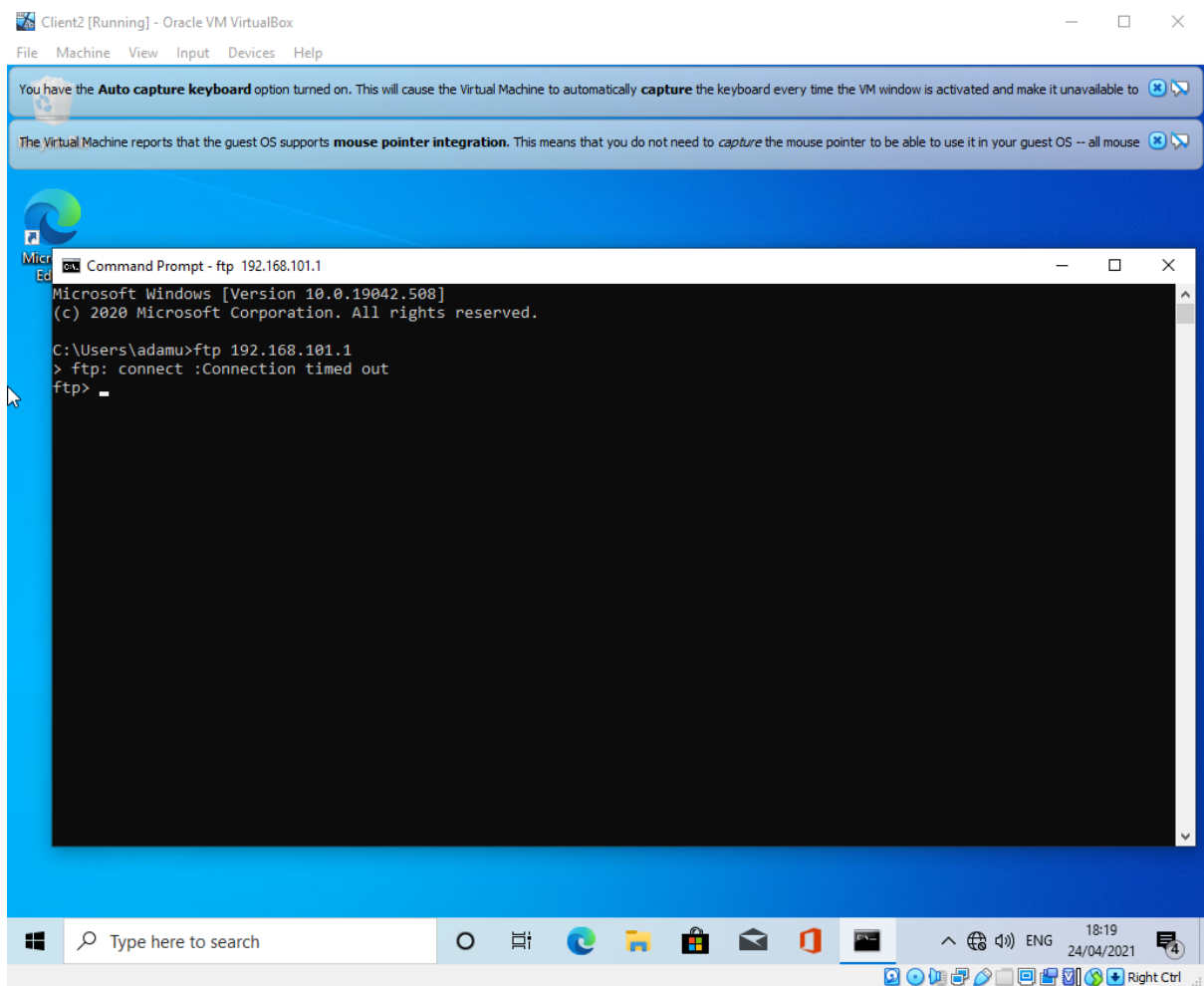


Figure 38 Evidence that client 2 is filtered out by the rule and cannot access FTP "server 2"



Worksheet 4

Task 3 Record your Observation:

3 a) How do Routers reference which networks they are able to connect to?

Routers are assigned an unchangeable public Wide Area Network (WAN) IP address by the ISP, but the router is in control of private Local Area Network (LAN) IP addresses, including its own[1]. When a device is connected to the router, the router will assign it a LAN IP address. The IP address serves as an identifier for the router[1]. The most common router configuration is to assign IP addresses through Dynamic Host Configuration Protocol (DHCP), where the device is assigned a dynamic IP address temporarily (usually 24 h)[2]. A new IP address will be assigned by the router for the same device if it reconnects at a later time. Alternatively, a device may be assigned a static IP address manually by the administrator[1].

IP addresses are grouped into subnets within networks[1]. The subnet determines the number of devices that may connect to the router: a common default setting for this is 250 devices[1]. The subnet mask tells the router how many devices may exist within its network, and allows traffic to be routed faster: the first part of the address relates to which subnet a device can be found in. A router with multiple interfaces will use the same process to determine all network connections[3].

Task 5: Failover Clustering for high availability systems/services

5 a) Give a detailed explanation of the concepts that need careful consideration when considering the usage of such a system. Also show one possible role within the Window Server OS environment that could provision these requirements. You should breakdown the aspects that need consideration when attempting to deploy this role/service. (Hint: Give screen shots of the role being configured and discuss these steps). **YOU DO NOT HAVE TO BUILD, DEPLOY OR TEST A FAILOVER CLUSTER.**

A failover cluster is a set of physical or virtual computer systems that work together to facilitate a High Availability (HA) or Continuous Availability (CA) environment for the applications and services that run within enterprise networks.

Failover clusters use multiple servers that are clustered together using cables and software[4]. Ideally, the servers and computers—and the software running on them—in the cluster should be identical or very similar. The clusters are constantly monitored for service functionality. If one component fails, then a failover occurs: the other components in the cluster take over from the failed component[4]. This ensures that when one component fails, the other components in the system will take over and provide an uninterrupted, or minimally-interrupted service. This is important for critical business applications, where even a small interruption may have serious repercussions.

Failover clusters also share access to a single storage volume, known as Cluster Shared Volumes[5]. This means that it is not necessary for drives to be dismounted and remounted during failover, ensuring that interruption is kept to a minimum.

Before deploying a failover cluster, all hardware and software should be checked for compatibility[6]. A failover cluster should share a storage device, but in a network with multiple failover clusters, each failover cluster should have its own storage that is inaccessible to other clusters on the network. Ideally, a network should use network adapter teaming or load-balancing in order to maximise performance on the network through managing bandwidth and traffic[6].

The Failover Cluster snap-in for Windows Server 2019 is one method of deploying a failover cluster. Active Directory Domain Services (AD DS) is used to create objects and roles for the failover cluster[6]. An administrator account is used to install the failover clustering feature to each component of the failover cluster. Each failover cluster should be added to its own Organisational Unit to ensure that Group Policy settings can be applied and controlled without interference[6]. The Failover Cluster Management tool should be used to run validation on the failover cluster to confirm that it is suitable. When this is complete, the failover cluster can be created in Server Manager.

Clustered roles, such as Namespaces or Hyper-V roles, can be created using the High Availability wizard[6].

Task 6: Observational Tasks

6 a) Assume that you are the Head - Network Administrator of an Enterprise Network which operates in multiple locations nationwide. Draft a network policy, Critical business applications high availability practices and security practices for your network. State all assumptions made. (Hint: In your draft, address (not limited to) the architecture/ topology/ design/ layout of the network, network access, security team, enforcement of security policies, analysis of security risks, scope of security changes (if needed), monitoring the security operations, mitigations in the event of violations, etc)

See attached.

Bibliography (1)

- [1] M. Horowitz, "IP addresses," *Router Security*, Dec. 2020.
<https://routersecurity.org/ipaddresses.php> (accessed May 04, 2021).
- [2] "Configuring the Cisco IOS DHCP Server." [Online]. Available:
www.cisco.com/go/cfn.
- [3] National Instruments Corp., "Best Practices for Using Multiple Network Interfaces (NICs) with NI Products," *ni.com*, Feb. 04, 2020. <https://www.ni.com/en-gb/support/documentation/supplemental/11/best-practices-for-using-multiple-network-interfaces--nics--with.html> (accessed May 14, 2021).
- [4] Microsoft, "Create a failover cluster," *Microsoft*, May 05, 2021.
<https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster> (accessed May 06, 2021).
- [5] Microsoft, "Use Cluster Shared Volumes in a failover cluster," *Microsoft*, May 05, 2021. <https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-cluster-csvs> (accessed May 06, 2021).
- [6] Microsoft, "Failover Clustering in Windows Server and Azure Stack HCI," *Microsoft*, Apr. 30, 2021. <https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview> (accessed May 06, 2021).

Enterprise Incorporated

Network security policy: Specifications, operations & mitigations

Audience: Technical Staff

Version 0.1 DRAFT

Table of contents

Table of contents	2
0. Foreword.....	4
1. Purpose	4
2. Network Specifications	4
2.1. Servers and hardware	4
2.1.1. Minimum technical requirements	4
2.1.2. Hardware monitoring.....	5
2.1.3. Server rooms.....	5
2.1.4. Use of network servers	5
2.1.4.1. General requirements for use.....	5
2.1.4.2. Backup requirements for servers.....	5
2.1.4.3. Logging requirements for servers	6
2.2. Software	6
2.2.1. Minimum technical requirements	6
2.2.2. Software monitoring	6
2.2.3. Critical business applications	6
2.2.3.1. List of critical business applications	7
2.2.3.2. High availability practices.....	7
2.3. Network access	7
2.3.1. Network hardware	7
2.3.2. Network change process.....	7
2.3.3. User accounts.....	7
2.3.3.1. Account creation	7
2.3.3.2. Account privileges	8
2.3.3.3. Account deletion	8
2.3.3.4. User training and responsibilities	8
3. Network security.....	8
3.1. Password policy.....	8
3.2. Firewalls	9
3.3. Security team	9
3.4. Security policy enforcement	9
3.4.1. Responsibilities	9
3.4.1.1. All Staff	9
3.4.1.2. Line managers	9

3.4.1.3.	Security team	10
3.4.1.4.	Security team senior management.....	10
3.4.1.5.	Chief Information Security Officer	10
3.4.2.	Enforcement.....	10
3.5.	Security risks	11
4.	Mitigations	11

0. Foreword

This document is an initial draft of the new Organisational Network Security Policy for circulation to Heads of Department and Technical Team members for first review.

The attention of Departmental Managers is drawn to Section 2.1: Critical Business Applications. If there are any applications in use in your department that you believe should be included in the Critical Business Applications that are not listed, please contact the Networks Team.

Comments and corrections should be directed to Adam Vimpany, Network Administrator.

1. Purpose

Enterprise Incorporated hold their duties to corporate governance in the highest regard. The security of our network infrastructure is of paramount importance to all areas of operation, and as such, a comprehensive security and networks policy has been implemented.

This policy is a technical document for use by members of the Networks and Security teams. The policy establishes the technical requirements of the networks infrastructure necessary to secure and protect corporate data. It covers all company network systems and hardware, both local and remote.

To ensure that the company network performs to the highest standards and meets legal requirements, Enterprise Incorporated follows the ISO/IEC 27000 series of standards for information security.

The term "*The company*" is used in this document to mean Enterprise Incorporated.

The term *administrator* is used in this document to mean a qualified Networks and Security technician who is authorised by the company to perform the duty described.

2. Network Specifications

2.1. Servers and hardware

2.1.1. Minimum technical requirements

All hardware procured must meet minimum standard requirements, in line with the company *Sustainable procurement policy*. They must meet all minimum technical and financial requirements, including those for performance, compatibility, security, affordability, scalability and future viability. Specification documents for common hardware and components, including, but not limited to, servers, personal computers, laptops and printers must be reviewed on a regular basis to ensure that they are still current and applicable.

2.1.2. Hardware monitoring

All hardware must be given equipment numbers and added to the assets register. The assets register must be audited on an annual basis to identify lost hardware.

Assets must be decommissioned in line with the company *Disposal of assets policy*. Data should be wiped from storage devices and the device physically destroyed to prevent data breaches.

Servers and system-critical computers and their components must be monitored on a regular basis to ensure functionality. Hardware components (RAM, CPU, etc.) must be replaced when they are reaching end-of-life or where monitoring indicates performance problems.

2.1.3. Server rooms

All server rooms must be equipped with suitable airflow and temperature and humidity controls[1]. Server room environmental control equipment must be serviced by an accredited engineer on a regular basis, according to manufacturer instructions.[2][1]. Server room environmental conditions must be logged and monitored daily to identify trends[2]. These logs must be retained according to the company *Retention policy*[2].

All servers must be equipped with uninterruptible power supply units, and all server rooms must be connected to an emergency backup generator in case of power failure[2]. Redundancy must be factored into the system[2].

2.1.4. Use of network servers

2.1.4.1. General requirements for use

All network servers should be tested and configured before being moved into and connected to the datacentre[2]. They must then be initialised and installed by an administrator using the Group Policy Management Console (GPMC) with the appropriate Group Policy Objects (GPO) in line with Standard operating procedure (SOP). [2].

Access to servers must be restricted in line with company security requirements[2]

All servers must be protected with a firewall.

Servers should be hardened in line with operating system guidelines. They must use the minimum hardware and software (ports, files, scripts, software etc.) necessary for functionality to prevent the introduction of security vulnerabilities.

2.1.4.2. Backup requirements for servers

Servers must be regularly backed up. Whole system or incremental backups must be made, according to server function.

The company *Disaster recovery* and *Data Backup policy* details the minimum backup requirements, including intervals, for both critical and normal servers on the network. RAID10 storage servers must be used for redundancy, and offsite backup data must be updated regularly.

A *golden image* of a disk must be made and sealed before major changes to a server are attempted.

2.1.4.3. Logging requirements for servers

Servers must have the means to perform fault, error and login logging, at a minimum, and these logs must be reviewed by the log management application on a regular basis. Logs should be retained in line with the company Retention Policy.

Critical servers, such as domain controllers or servers that contain sensitive data or Critical Business Applications, must have mitigation and disaster recovery plans in place for system failure. The mitigation and disaster recovery plans for critical servers supersede this document.

2.2. Software

2.2.1. Minimum technical requirements

Software used by the company must be licensed. Licenses for software must be kept securely.

Requests for new software must be made to the Networks and Security team and approved by senior staff. Software that has not been authorised for use must not be used or downloaded onto the company network.

All new software, or updated software must be checked for compatibility and security by a qualified administrator on a test server before roll-out to other devices. Software with known vulnerabilities or compatibility problems must never be used on the network.

Software must only be installed by an administrator using the GPMC, and then allocated to relevant GPOs. Software must be assigned or published to computers or servers, not users, wherever possible.

2.2.2. Software monitoring

The Networks and Security team must monitor for security alerts and known vulnerabilities of all company software, both prior to installation and during use.

The Networks and Security team must monitor for software updates and patches. Updates that address vulnerabilities must be installed and rolled out using the GPMC as soon as is practicable.

Error and login logs (at a minimum) for relevant software must be created, and these logs must be reviewed by the log management application on a regular basis. Logs should be retained in line with the company Retention Policy.

2.2.3. Critical business applications

All critical business applications should be identified and monitored by the Networks and Security team. Departmental managers should flag any critical business applications used in their departments to the Networks and Security team.

2.2.3.1. List of critical business applications

- Network shared storage: very high criticality
- Financial trading system: very high criticality
- Customer database: very high criticality
- Internal messaging system: high criticality
- Internal human resources management system: medium criticality

2.2.3.2. High availability practices

High availability practices are essential for the delivery of business continuity. Business critical applications must be consistently accessible to all users on the network, with no downtime.

See section 4.1 for mitigations implemented by The Enterprise Incorporated network for all business critical applications.

2.3. Network access

Access to the network must be authorised and restricted in accordance with ISO/IEC 27000:2018[3].

2.3.1. Network hardware

2.3.2. Network change process

All changes to the network must be requested and documented through the IT Service Management process. Change requests must be approved by the networks and security department administrators before action, excepting only changes that fall under the *Disaster recovery* policy in case of serious system failure.

2.3.3. User accounts

All users of the network must be assigned their own individual user account with a password. Users must not allow other people to use their account or share their password.

2.3.3.1. Account creation

New accounts for employees must be requested in writing by department managers and approved by networks and security administrators. Persons not employed by the organisation may be granted a temporary account in exceptional circumstances (e.g. contractors) only with the express permission of the Head of Networks and Security.

Accounts must be created and added to appropriate GPOs by an administrator using the GPMC.

2.3.3.2. Account privileges

User accounts must be added to a GPO with the fewest privileges that will suffice for their job role and seniority. Requests for enhanced privileges must be requested in writing, together with justification, to the networks and security administrators by senior staff, and approval granted by networks and security administrators.

Account privileges and GPOs must be reviewed annually by both networks and security administrators and Heads of Department to ensure they are still appropriate. Unnecessary privileges must be revoked.

Administrators must follow the Microsoft *Account, Global, Universal, Domain Local, Permission* (AGUDLP) recommendations for all user account permissions.

2.3.3.3. Account deletion

Unused accounts will be suspended after 120 days. Temporary accounts will be suspended after 120 days. All suspended accounts will be reviewed on a regular basis by an administrator and deleted if appropriate.

Department managers must inform network and security administrators of changes in employment for their staff immediately so that privileges can be revoked or amended, and accounts deleted promptly if required in order to prevent unauthorised access to the network.

2.3.3.4. User training and responsibilities

All new starters at the organisation must undergo an Information and Technology induction, and agree to abide by the terms of the organisation security and acceptable use policies before they are granted access to the network. They will be made aware of their responsibilities to data security through participation on statutory training courses.

3. Network security

The company follows the requirements for information security management systems (ISMS) as set out in ISO/IEC 27000:2018[3].

3.1. Password policy

All users agree to abide by the organisation *Password policy*.

User passwords must be a minimum of eight characters long[4]. Users are encouraged to create a memorable, long, complex passphrase, but this is not enforced by the network. A password strength meter and password blacklist are implemented at password-creation to encourage the use of safe passwords and prevent use of very weak passwords (e.g. “password” or similar)[4].

The organisation prevents DDOS or brute-force attacks by using rate-limiting mechanisms[4].

Passwords are hashed using one-way key derivation functions (KDF)[4].

3.2. Firewalls

The company firewall is a hardware-based network firewall that is used to protect the network from external threats[5]. The physical network ports are configured to control access to servers and other network resources, whilst isolating each of the different areas of the network[5].

The physical network ports are configured to control access to servers and other network resources, whilst isolating each of the different areas of the network[5]. This ensures that security threats are contained and cannot spread to other areas of the network[5].

3.3. Security team

The security team are appointed by the company management board, and each of the roles and responsibilities required by ISO 27001 are divided amongst the senior staff[6].

The Chief Information Security Officer has direct oversight of the information security team[6].

Incidents and events must be reported to the security team in line with the requirements of ISO 27001[6]. Lines of reporting are detailed in the *Incident management* policy, which details the staff members responsible for the investigation, monitoring and correction of security incidents or near-misses[6].

3.4. Security policy enforcement

3.4.1. Responsibilities

3.4.1.1. All Staff

All staff have a responsibility to report all security incidents, near-misses and areas of concern to the security team when they occur.

All staff have a responsibility to abide by the terms of company policy, including security policy, and ensure their statutory training is complete and up to date.

Agreement and compliance with company policy is a condition of employment.

3.4.1.2. Line managers

Line managers are responsible for ensuring that their staff comply with company policy in all areas, including security policy. In the first instance, line managers must ensure compliance with statutory training, such as information governance training, and that company policies have been read, understood and agreed to by their staff.

Line managers must keep a secure record of staff agreements to abide by policy[7].

Line managers must review compliance with all company policy regularly, and report and record non-compliance. Minor non-compliance (for example, a staff member exceeding the renewal date of their statutory training) can be dealt with by line managers. Major non-compliance with security policy must be reported to the security team senior management.

3.4.1.3. Security team

The security team are responsible for monitoring use of the network and identifying suspected security breaches, non-authorised modifications or access, or non-compliance.

The security team is responsible for the performance of logging and monitoring tasks to aid in the above[7].

The security team are responsible for investigation of any incident reports or near-misses raised by staff, in accordance with the *Incident management* policy, and under the guidance of the appropriate senior staff member.

The security team are responsible for implementing necessary changes to the network, in accordance with change management procedures.

The security team are responsible for alerting senior management to security breaches, areas of concern or non-compliance.

3.4.1.4. Security team senior management

The senior management staff are responsible for reviewing, monitoring and managing company compliance to ISO 27001:2013.

Senior management staff must ensure that staff training programs are available and appropriate for staff, and review this regularly[7].

Senior management staff are responsible for arranging external auditors to review compliance to ISO 27001:2013[6].

Senior management staff are responsible for managing investigation of non-compliances and implementing corrective actions. They must implement proactive security policy and monitor effectiveness of these policies.

Senior staff must participate in monthly management reviews and internal audits[7].

3.4.1.5. Chief Information Security Officer

The Chief Information Security Officer holds ultimate decision-making authority for information and networks security matters.

3.4.2. Enforcement

Line managers have responsibility for ensuring compliance with policy and training within their team. Minor non-conformances may be dealt with informally but must be recorded or reported. Line managers must escalate non-conformances and incidents that do not fall within their remit in accordance with the *Incident management* policy.

Serious or malicious breaches of security by staff members will be dealt with under the company *Disciplinary* policy. Staff will not be disciplined for accidental infection of equipment with viruses etc., except in the case of serious negligence, deliberate misuse or malicious intent.

Enforcement action must be taken in accordance with the *Incident management* policy. The *Incident management* policy sets out circumstances under which security incidents must be escalated for further enforcement action: for example, incidents where company legal counsel must be consulted, law enforcement must be involved, or where the company has obligations to report under the Data Protection Act 2018[6].

3.5. Security risks

Risk reviews are performed as part of the annual management review, to identify areas of concern[6].

Risk reviews are performed on a monthly basis for business-critical applications and high-likelihood high-impact infrastructure. Low-impact risk assets will have a risk review annually.

4. Mitigations

The Enterprise Incorporated network has two datacentres: the Swansea datacentre and the Cambridge datacentre. The datacentres are in an active-active configuration to ensure business continuity.

Business critical applications are hosted across multiple servers across both datacentres. Each server will be automatically backed up in accordance with the *Data Backup policy*.

Application server requests to the datacentres are handled by hardware-based load-balancers, which ensure that requests are distributed efficiently between datacentres and servers. When there is high-volume traffic, requests that time-out will be diverted automatically to the other datacentre, thereby maximising availability and performance.

For business critical database servers, the replication system ensures that the data held on the primary database server is replicated onto the secondary server. The two-node clustered failover cluster monitors for service disruption. Requests are routed to the secondary server in the event of primary server failure in order to ensure business continuity.

5. Bibliography

- [1] H. Liu, Y. Kuang, C. Liu, L. Xiao, and G. Xu, "DESIGN OF DATA CENTER'S HIGH RELIABILITY IN LARGE AGRICULTURAL ENTERPRISE."
- [2] International Organization for Standardization, "ISO/IEC 30134-1:2016 Information Technology — Data centres — Key performance indicators — Part 1: Overview and general requirements," ISO/IEC 30134-1:2016, 2016
- [3] International Organization for Standardization, "ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary," ISO/IEC 27000:2018(en), 2018
- [4] "Digital Identity Guidelines: Authentication and Lifecycle Management," *Special Publication (NIST SP) - 800-63B*, 2017, doi: 10.6028/nist.sp.800-63b.
- [5] H. Andrea, "Network based Firevall vs Host based Firewall - Discussion and Comparison," *Networks Training*, 2021. <https://www.networkstraining.com/network-based-firewall-vs-host-based-firewall-discussion-and-comparison/> (accessed May 04, 2021).
- [6] International Organization for Standardization, "ISO/IEC 27001:2013 Information Security Management," ISO/IEC 27001:2013, 2013
- [7] P. Biswas, "ISO 27001:2013 A.6 Organization of information security," *ISO Consultant in Kuwait*, 2019. <https://isoconsultantkuwait.com/2019/12/25/iso-270012013-a-6-organization-of-information-security/> (accessed May 04, 2021).