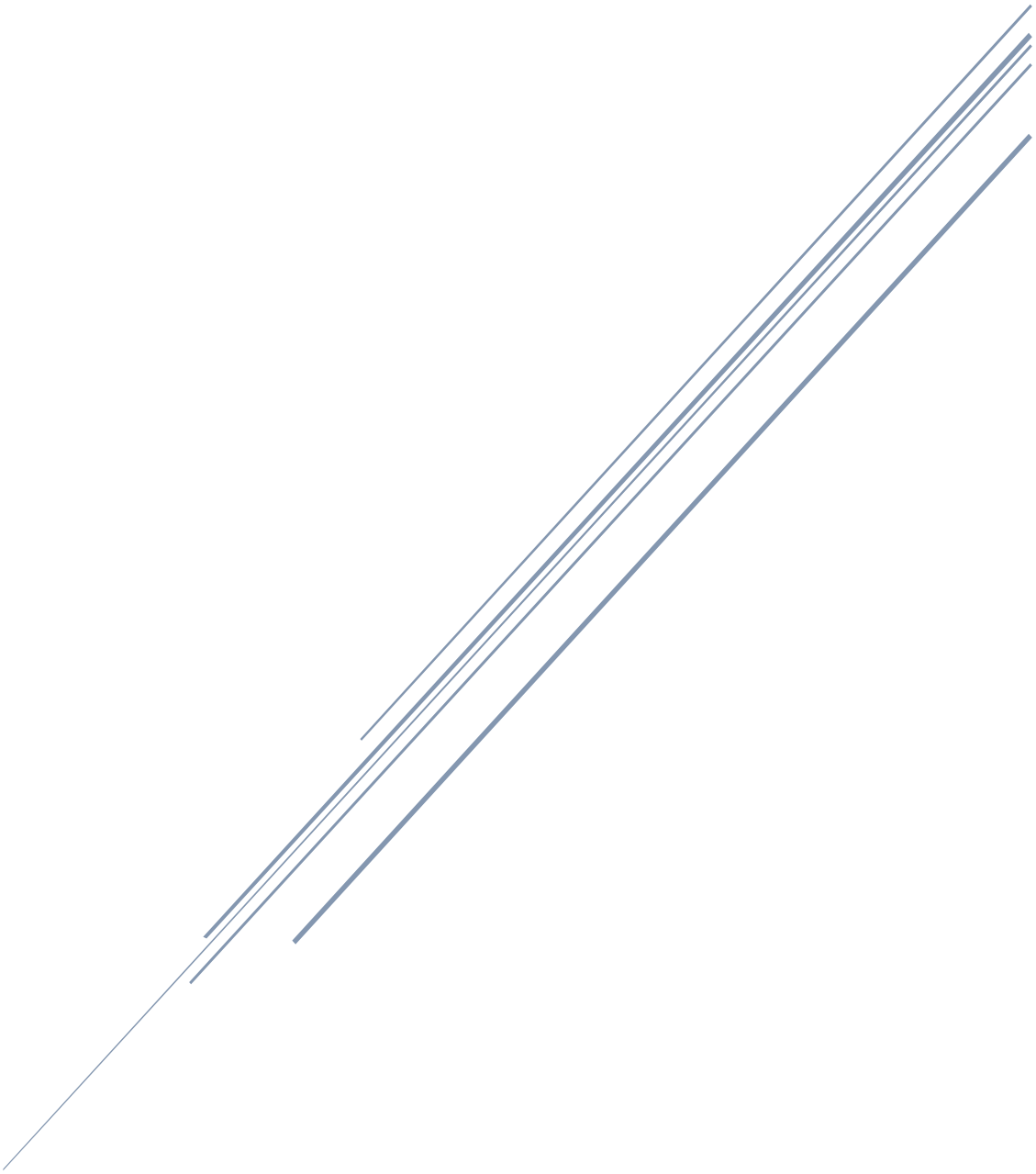
R&D REPORT: CONFIGURATION OF A SITE-TO-SITE (S2S) VPN USING HYPER-V

Author: Virat Pandey



1. Objective

This document provides a step-by-step guide on how to install and configure the Routing and Remote Access Service (RRAS) on a Windows Server 2019 machine. The goal is to configure the server to act as a Network Address Translation (NAT) router, allowing multiple client devices on a private network to access the internet through a single public IP address.

---

2. Prerequisites

Before installing RRAS, the server must be correctly configured with the necessary hardware and network settings.

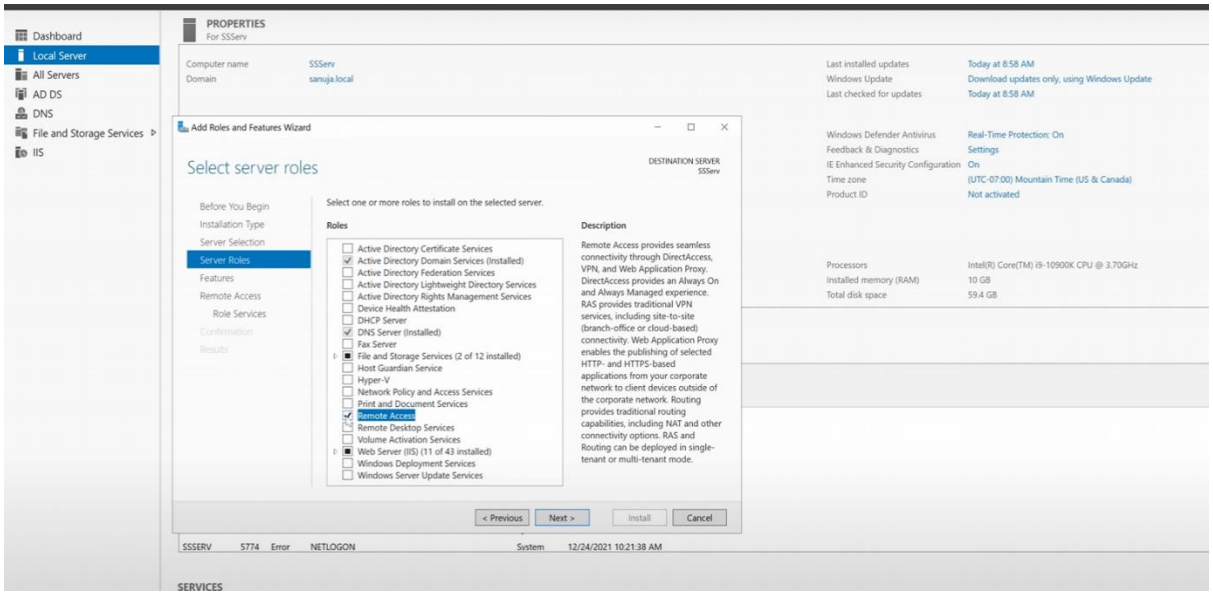
1. Network Adapters: A minimum of two network interface cards (NICs) are required.
    - External NIC: One NIC must be connected to the external network (the Internet). This adapter can be configured with DHCP to automatically receive an IP address.
    - Internal NIC: The second NIC must be connected to the private, internal network segment. This adapter requires a static IP address to act as the default gateway for internal clients.
2. IP Configuration:
    - The internal NIC was configured with a static IP address of 192.168.1.3 and a subnet mask of 255.255.255.0. The DNS server was set to point to itself (192.168.1.3).

---

3. Phase 1: Installing the Remote Access Role

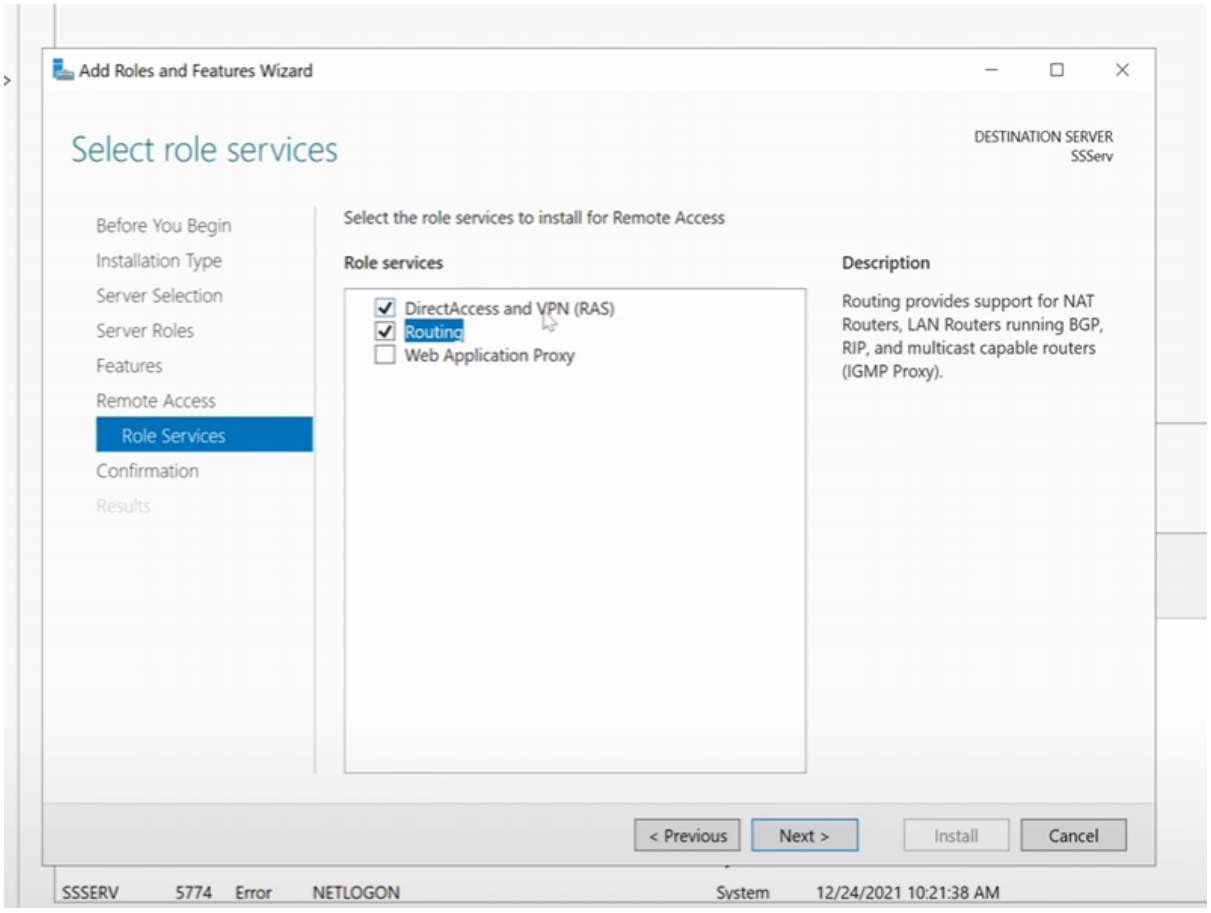
The RRAS functionality is added to Windows Server by installing the "Remote Access" server role.

1. Add Roles and Features: From the Server Manager dashboard, the "Add Roles and Features" wizard was initiated from the "Manage" menu.
2. Role Selection: After proceeding through the initial wizard pages, the "Remote Access" role was selected from the list of available server roles.

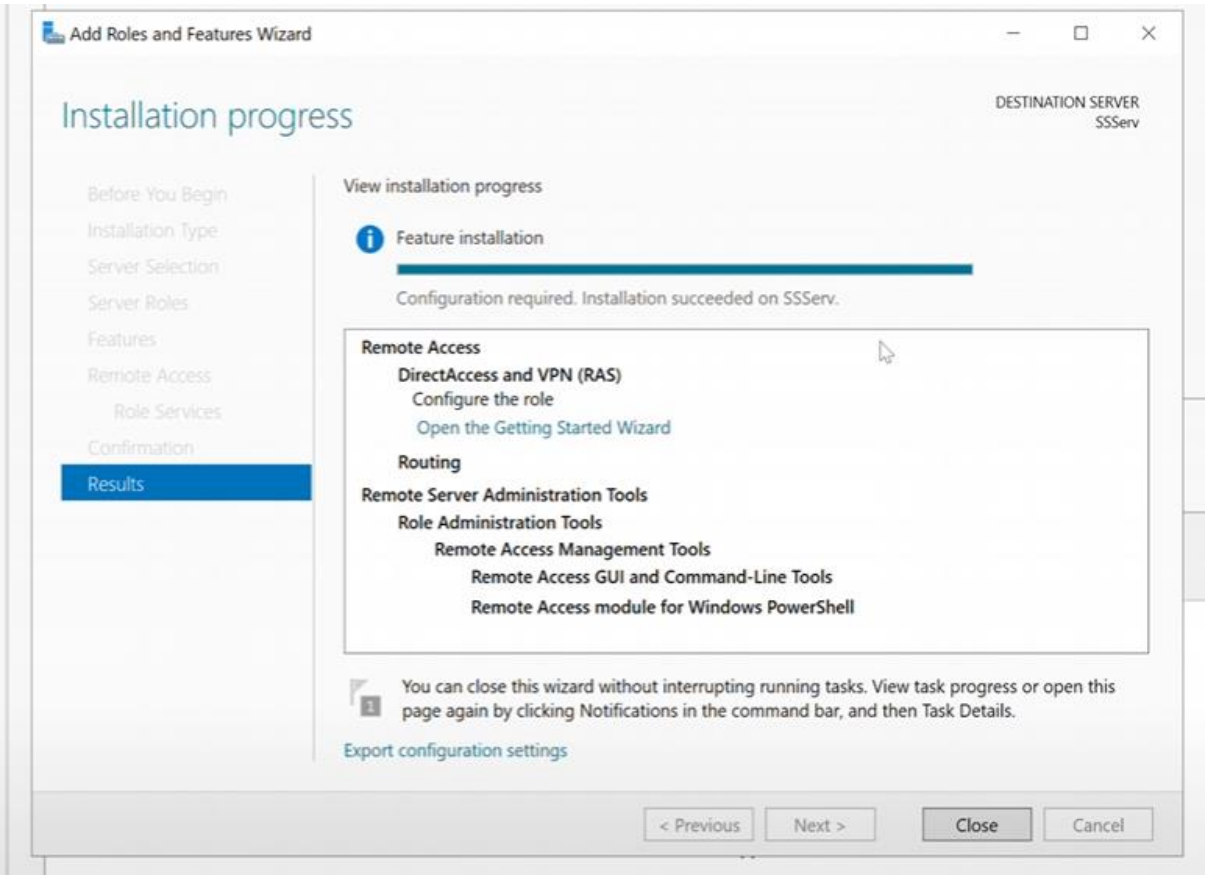


.

3. Role Service Selection: Within the Remote Access role services, the "Routing" option was selected. This automatically included the "DirectAccess and VPN (RAS)" services as a dependency.



4. Installation Confirmation: The installation was confirmed, with the option to automatically restart the server if required.

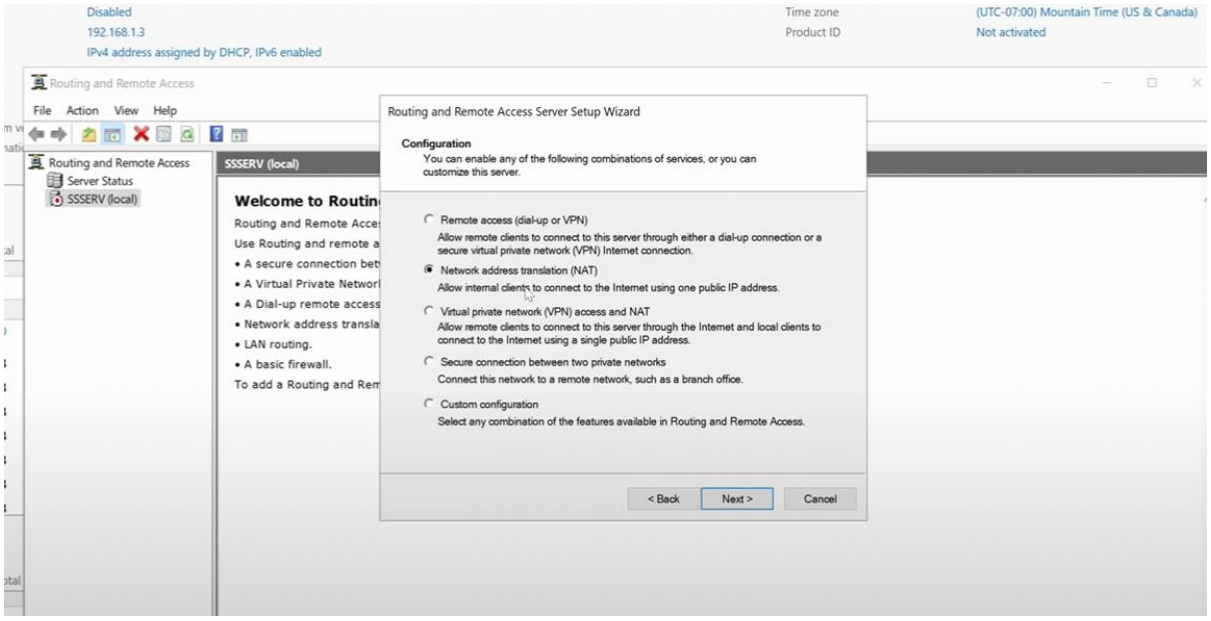


---

5. Phase 2: Configuring RRAS for NAT

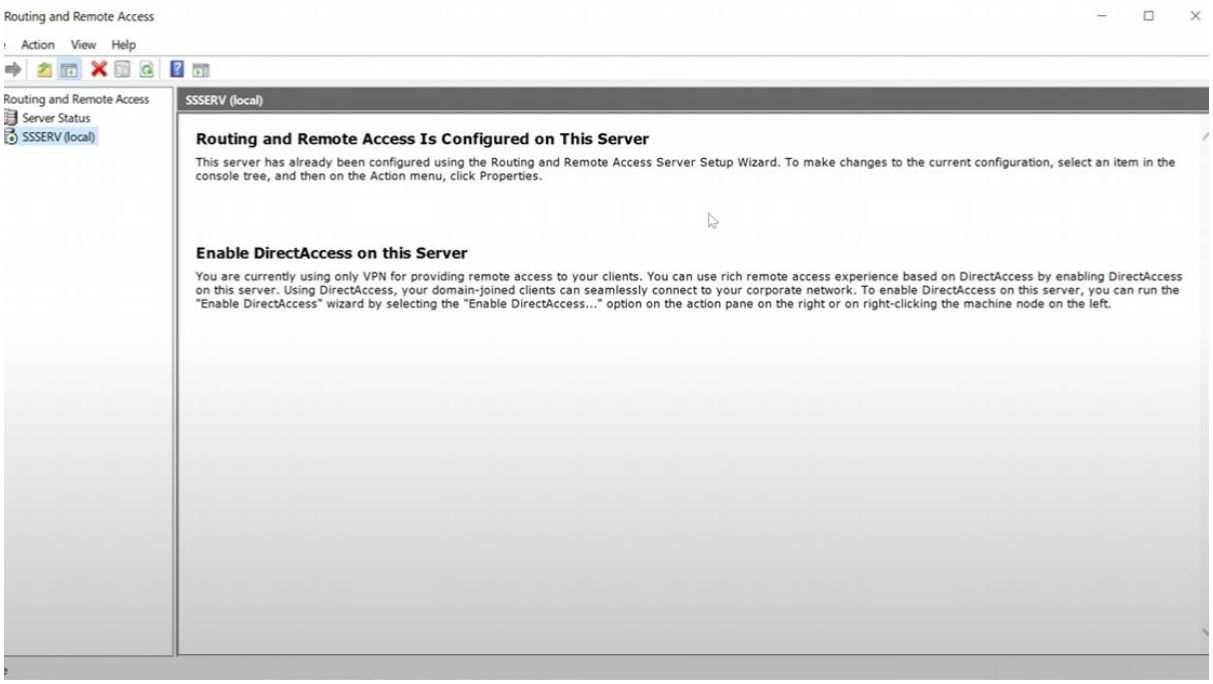
Once the role is installed, the Routing and Remote Access service must be configured.

1. Launch RRAS Console: The "Routing and Remote Access" management console was opened from the "Tools" menu in Server Manager.
2. Configuration Wizard: Inside the RRAS console, right-clicking the server name and selecting "Configure and Enable Routing and Remote Access" launched the setup wizard.
3. NAT Configuration: The "Network Address Translation (NAT)" option was selected. This configuration allows internal clients to connect to the internet using the server's single public IP address.



.

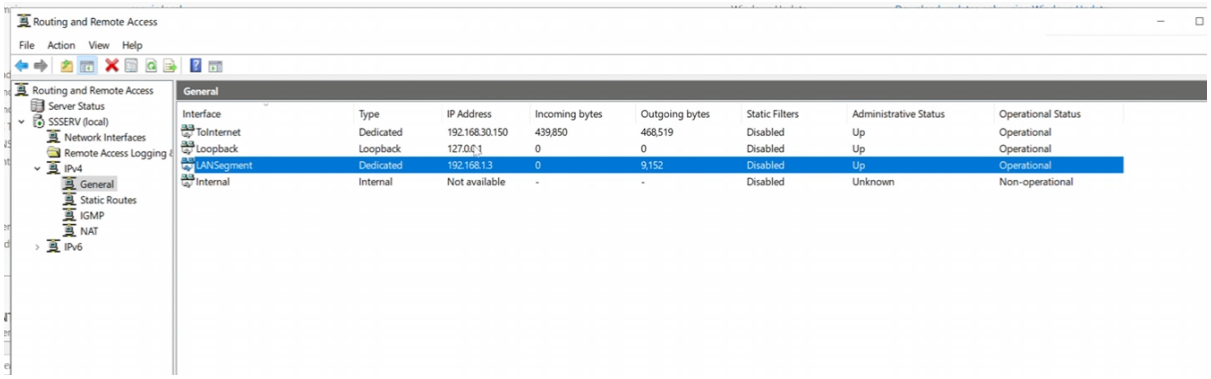
4. Public Interface Selection: The wizard prompted for the selection of the public-facing network interface. The NIC connected to the internet was chosen.
5. Finalization: The wizard was completed, and the RRAS service was started.



5. Phase 3: Verification

After configuration, the RRAS console shows a green "up" arrow on the server icon, indicating the service is running correctly.

To test functionality, a web browser was opened on the server to access an external website. The data counters for the "To the Internet" interface in the RRAS console were observed to increase, confirming that internet traffic was successfully passing through the newly configured NAT router.



---

6. Conclusion

The Routing and Remote Access Service (RRAS) was successfully installed and configured on Windows Server 2019 to function as a NAT router. The process involved ensuring prerequisite network configurations were in place, installing the appropriate server role and services, and completing the configuration wizard. Verification tests confirmed that the server is now capable of routing traffic from a private network to the public internet, providing a foundational component for more complex network setups.