Assignment - 8

Site to Site

Prepare R&D Document on How to setup Site to Site using Hyper-V

Ananya Srivastava
CLOUD INFRA

Table of Content

1. Introduction

In the contemporary landscape of digital infrastructure, organizations often require the seamless interconnection of multiple physical sites, data centers, or cloud environments. A Site-to-Site Virtual Private Network (VPN) is a vital technology that facilitates secure and reliable connectivity between distinct network locations over the internet. By leveraging Hyper-V, Microsoft's virtualization platform, administrators can effectively configure and manage Site-to-Site VPNs to ensure that resources across different sites can communicate securely and efficiently.

Hyper-V allows for the creation of virtualized environments that can host virtual machines (VMs) running various services, including networking and VPN solutions. By utilizing Hyper-V's capabilities, organizations can set up a virtualized network infrastructure that supports Site-to-Site VPN connections. This approach not only optimizes hardware utilization but also enhances the flexibility and scalability of network management.

Setting up a Site-to-Site VPN using Hyper-V involves several critical steps. Initially, Hyper-V must be configured to host the necessary virtual machines that will act as VPN gateways. These VMs will be responsible for establishing and maintaining the VPN tunnels between sites. The configuration process includes setting up virtual networks within Hyper-V to simulate the physical network environment.

Once the virtual network is in place, the next step is to configure the Routing and Remote Access Service (RRAS) on the VPN gateway VMs. RRAS is a Microsoft service that provides routing, remote access, and VPN capabilities. By configuring RRAS, administrators can define the VPN connections, routing protocols, and security settings required for the Site-to-Site VPN.

After configuring RRAS, the actual Site-to-Site VPN connection needs to be established. This involves specifying the VPN type, authentication methods, and IP address assignments for the VPN gateways. By defining these parameters, the VPN gateways can securely connect and route traffic between the sites.

Testing the VPN connection is crucial to ensure that the setup is functioning as expected. Administrators need to verify that the VPN tunnels are established correctly and that data can flow seamlessly between the connected sites. This step may involve troubleshooting common issues such as connectivity problems, routing errors, and authentication failures to ensure a robust and reliable VPN setup.

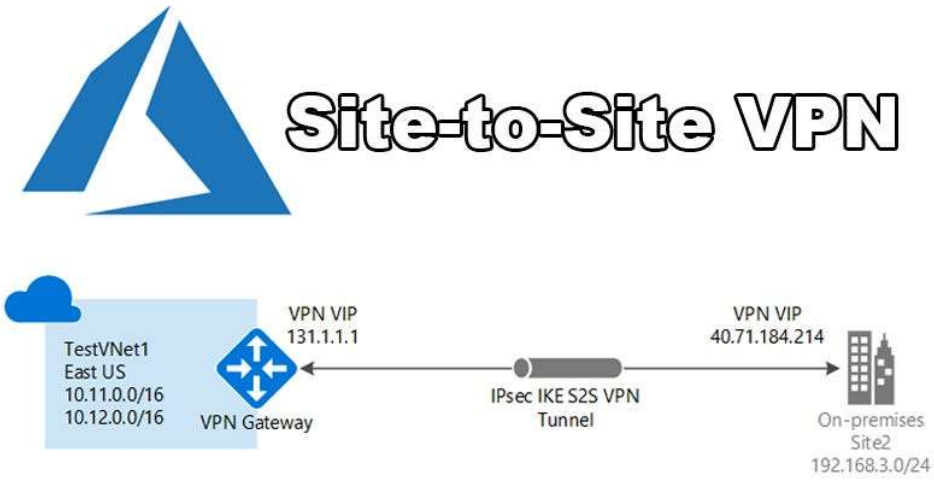
2. Prerequisites

Before setting up a Site-to-Site VPN using Hyper-V, ensure you have the following:

- A physical or virtual server running Windows Server with Hyper-V enabled.
- Administrative access to the Hyper-V Manager.
- Two virtual machines to act as VPN gateways.
- Basic understanding of networking concepts and VPN protocols.
- IP address ranges for the local and remote networks.

3. Network Diagram

A network diagram can help visualize the Site-to-Site VPN setup.



---

4. Step-by-Step Configuration

Configuring Hyper-V Virtual Machines

1. **Create Virtual Machines**:
   - Open Hyper-V Manager.
   - Create two virtual machines, one for each VPN gateway.
   - Assign appropriate resources (CPU, memory, storage) to each VM.

Setting Up the Virtual Network in Hyper-V

1. **Create Virtual Switches**:
   - In Hyper-V Manager, create virtual switches for each network.
   - Configure internal or external switches based on your network design.
2. **Connect VMs to Virtual Switches**:
   - Connect the VPN gateway VMs to the appropriate virtual switches.
   - Ensure network connectivity between the VMs and the respective networks.

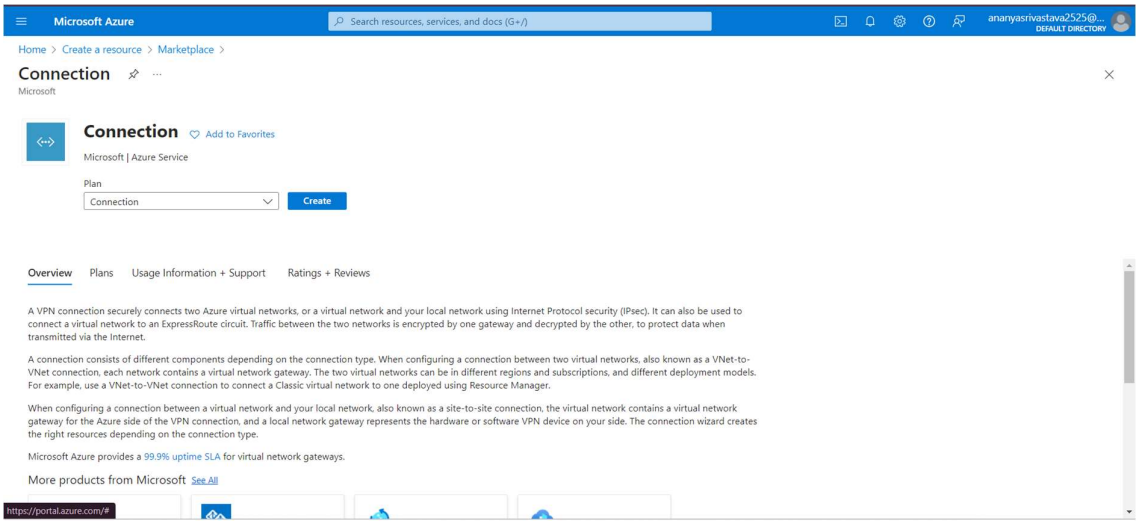
Configuring Routing and Remote Access Service (RRAS)

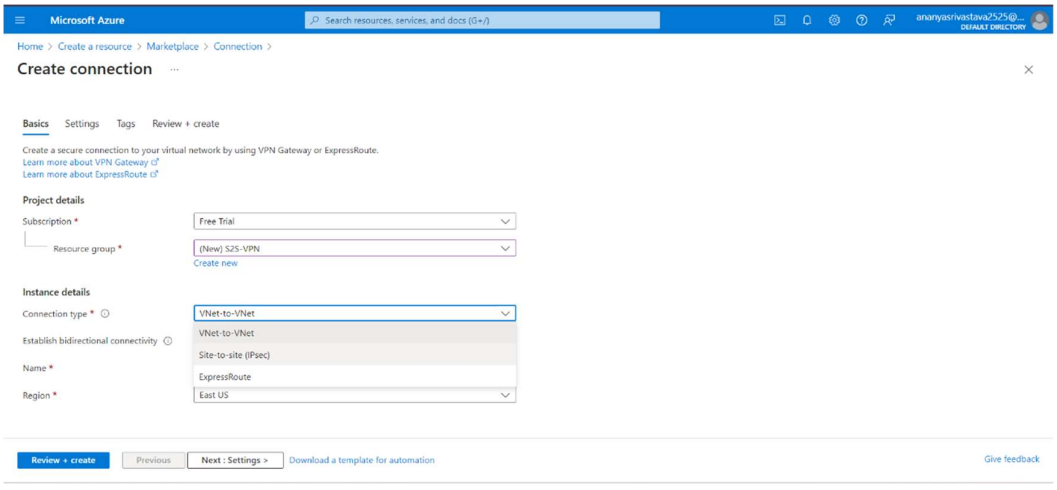
1. **Install RRAS**:
   - On each VPN gateway VM, open Server Manager.
   - Add the "Remote Access" role and include the "Routing" role service.
2. **Configure RRAS**:
   - Open the RRAS console.

- Right-click the server name and select "Configure and Enable Routing and Remote Access".
- Choose "Custom configuration" and select "VPN access" and "LAN routing".

Configuring the Site-to-Site VPN Connection

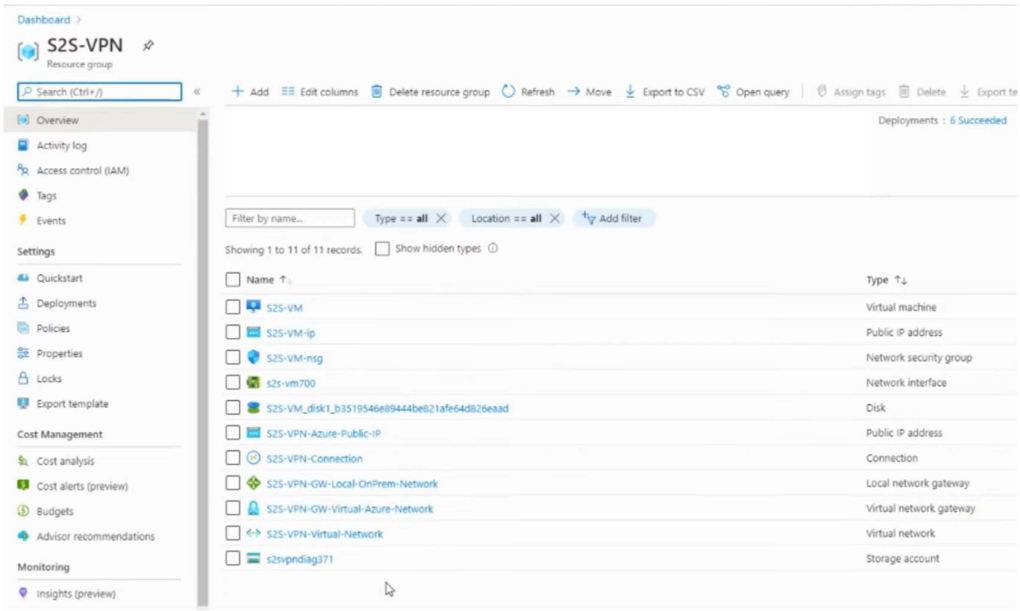
1. **Define VPN Interfaces**:
   - In the RRAS console, add new demand-dial interfaces.
   - Specify the connection type as "VPN" and choose the appropriate VPN protocol (e.g., L2TP, PPTP).
2. **Configure Authentication and IP Address Assignment**:
   - Set up authentication methods (e.g., pre-shared key, certificate).
   - Configure IP address assignment for the VPN connection.





Testing the VPN Connection

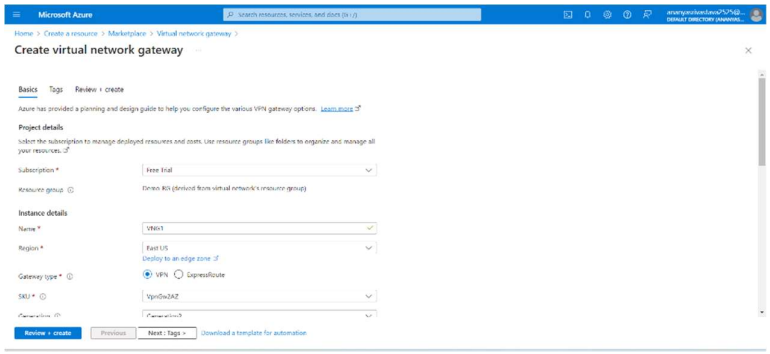
1. **Verify VPN Tunnel**:
   - Ensure that the VPN tunnel is established between the local and remote sites.
   - Use ping tests and other network utilities to verify connectivity.
2. **Check Data Flow**:
   - Ensure that data can flow between the networks without issues.
   - Troubleshoot any connectivity or routing problems.



5. Hands-on Implementation

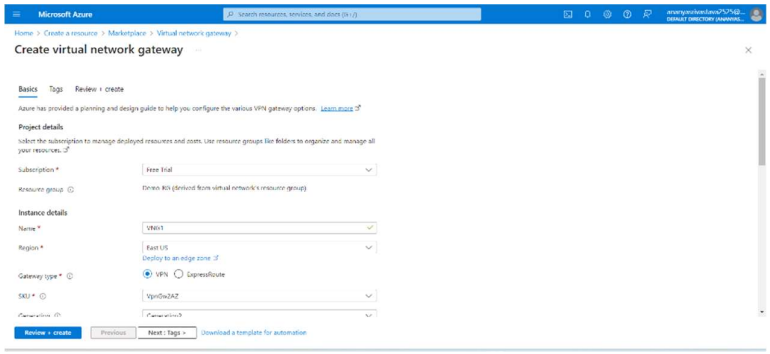
Configuring VPN Gateway

1. **Create VPN Gateway in Azure**:
   - In the Azure portal, navigate to "Create a resource" > "Networking" > "Virtual network gateway".
   - Fill in the necessary details such as Name, Region, Gateway type (VPN), VPN type (Route-based), SKU, Virtual Network, Public IP address.
   - Click "Review + create" and then "Create".



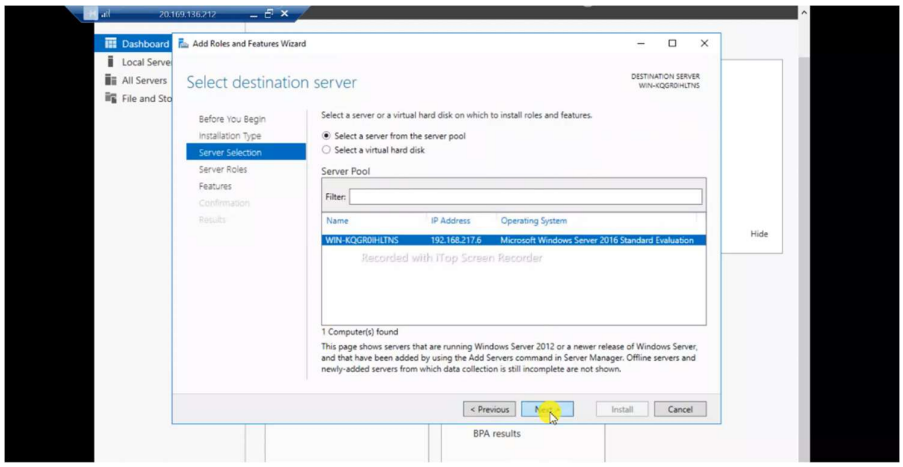
Configuring Local Network Gateway

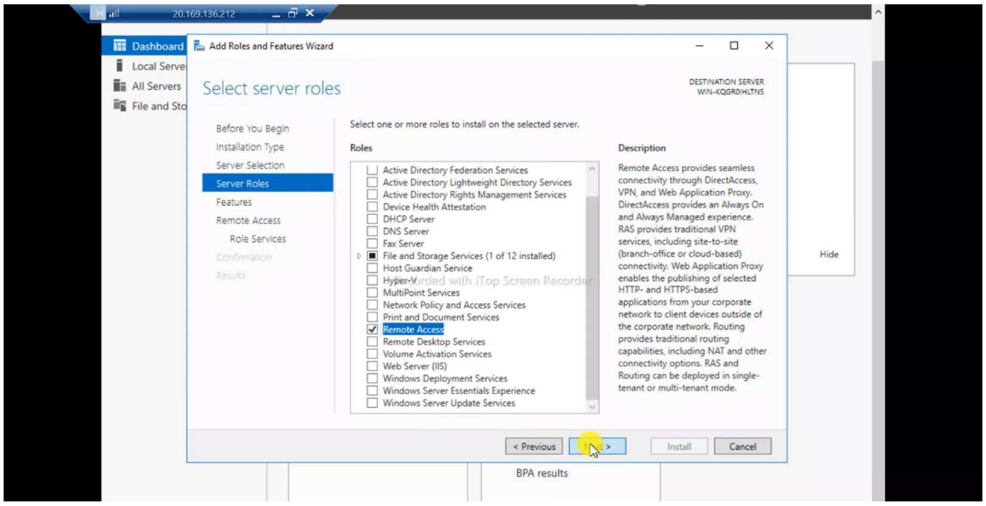
1. **Create Local Network Gateway**:
    - In the Azure portal, navigate to "Create a resource" > "Networking" > "Local network gateway".
    - Provide the necessary details such as Name, IP address of the on-premises VPN device, and Address space that defines the range of IP addresses for the local network.
    - Click "Review + create" and then "Create".

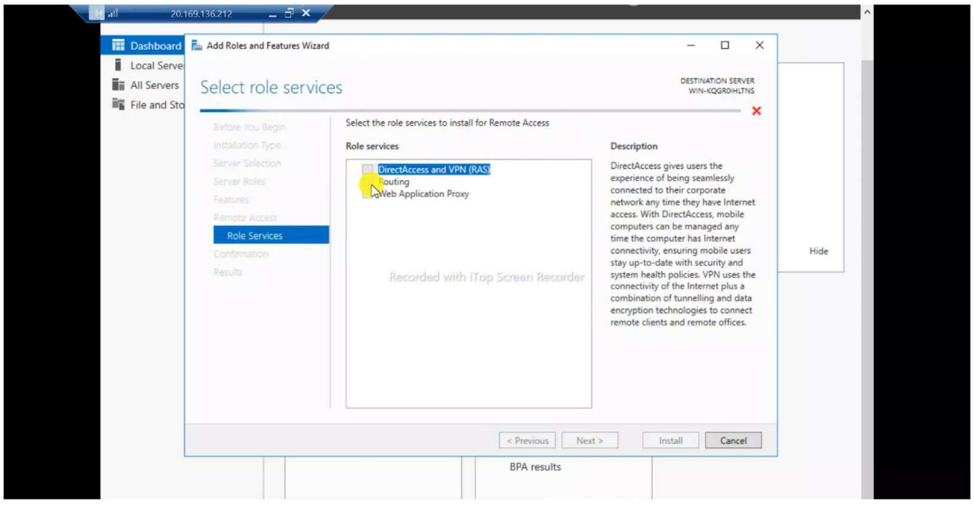


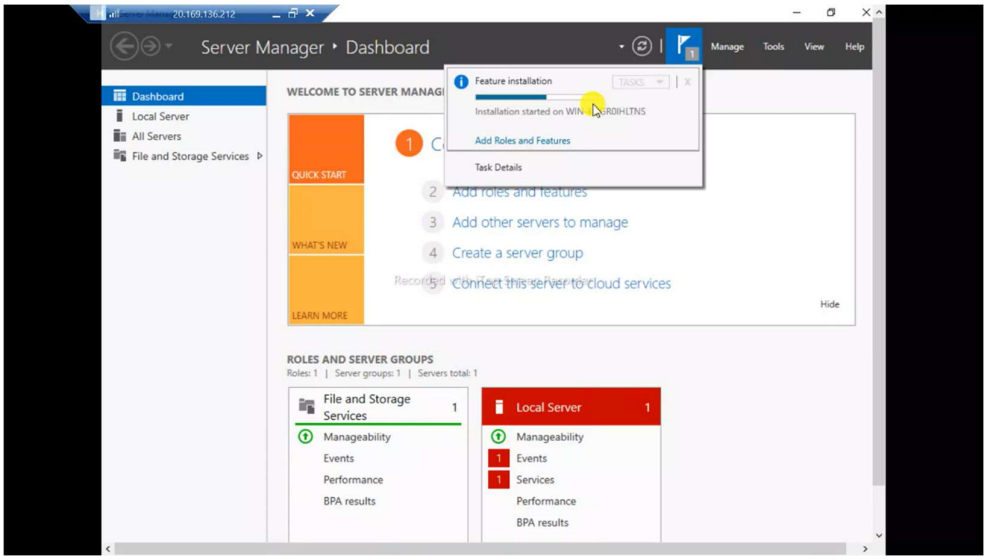
Implementing Encryption Mechanisms

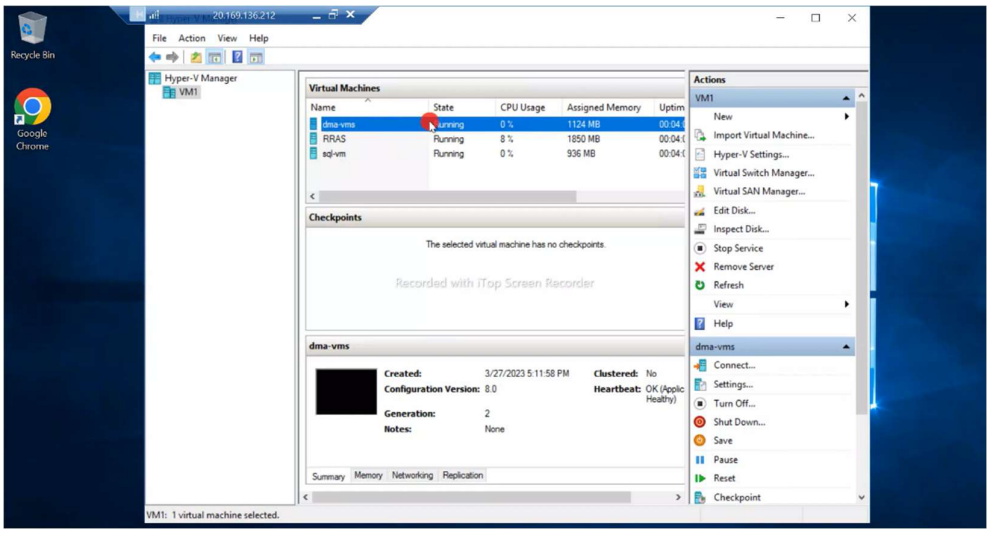
1. **Configure Encryption Settings in RRAS**:
    - In the RRAS console, navigate to the properties of the VPN connection.
    - Go to the Security tab and configure the encryption settings (e.g., AES256).
    - Ensure that both VPN gateways have matching encryption settings.


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-KQGR0IHLTNS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-KQGR0IHLTNS
192.168.217.6
Microsoft Windows Server 2016 Standard Evaluation
Recorded with iTop Screen Recorder
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
BPA results
Hide


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-KQGR0IHLTNS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Description
Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
Recorded with iTop Screen Recorder
< Previous
Next >
Install
Cancel
BPA results
Hide


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-KQGR0IHLTNS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
DirectAccess gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, mobile computers can be managed any time the computer has Internet connectivity, ensuring mobile users stay up-to-date with security and system health policies. VPN uses the connectivity of the Internet plus a combination of tunnelling and data encryption technologies to connect remote clients and remote offices.
Recorded with iTop Screen Recorder
< Previous
Next >
Install
Cancel
BPA results
Hide





2. **Set Up IPsec in Azure**:
   - In the Azure portal, navigate to the VPN connection properties.
   - Configure the IPsec/IKE policy with the desired encryption and integrity algorithms.

5. Troubleshooting

- **Common Issues**:

  • VPN tunnel not establishing: Verify VPN settings and authentication methods.
  • Routing issues: Check routing tables and ensure correct IP configurations.

• Connectivity problems: Ensure virtual switches and network adapters are correctly configured.

6. Conclusion

Setting up a Site-to-Site VPN using Hyper-V provides a robust solution for securely connecting multiple sites. By following the detailed steps outlined in this document, administrators can successfully configure and manage a Site-to-Site VPN, ensuring secure and reliable communication between distinct network locations.

7. References

- Hyper-V documentation
- RRAS documentation
- VPN configuration guides
- YouTube : https://youtu.be/LWg4sJENIYo?si=X63VK92bM_M_KD8D
- Website: https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal
- Website: https://www.google.com/search?sca_esv=613c3e8cf9f502a0&sca_upv=1&q=site+to+site+azure&tbm=isch&source=lnms&fbs=AEQNm0AyvaLQ3NL66YfFpz1Ee77Y907IdzVHuwZKSxTUG42099UCERtnFqShFWb9UVlyB-mvWARawr-kd-SaSXcafzegaQpu7lls0oyMLzZPe7IubW7xbEL5pZXynGD8jRIshNu-dI-63aa1ozw_Rx0sDSB6SSJQtpJH9aXKhnVsxGstQdpcrjlHHnm6SD6fZLWsgKcRpDJc&sa=X&sqi=2&ved=2ahUKEwjEwrW10o2HAxWdTmwGHaHjDmQQ0pQJegQIEhAB&biw=1536&bih=695&dpr=1.25#imgrc=LT8tILAXYMDRyM 3