Azure

- Make user member of a dynamic group based on a secondary group membership
- G-Suite (Google Workspace) authentication into Office 365 (SAML)
- Create Dynamic Group for all licensed Users
- Creating a Secure Site-to-Site VPN Connection in Azure: A Step-by-Step Guide
- Microsoft License Plan Reference

Make user member of a dynamic group based on a secondary group membership

```
user.memberof -any (group.objectId -in ['group1-123-123-123','group2-123-123-123'])
```

G-Suite (Google Workspace) authentication into Office 365 (SAML)

https://www.youtube.com/watch?v=C46djGWiaDA

https://pastebin.com/buTh1mcm

1. Install-Module MSOnline
2. Import-Module MSOnline
3. Connect-MsolService
4. $domainName = "<your domain>"
5. [xml]$idp = Get-Content <metadata-xml-file-path>
6. $activeLogonUri = "https://login.microsoftonline.com/login.srf"
7. $signingCertificate = ($idp .EntityDescriptor.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509Data.X509Certificate | Out-String).Trim()
8. $issuerUri = $idp.EntityDescriptor.entityID
9. $logOffUri = $idp.EntityDescriptor.IDPSSODescriptor.SingleSignOnService.Location[0]
10. $passiveLogOnUri = $idp .EntityDescriptor.IDPSSODescriptor.SingleSignOnService.Location[0]
11. Set-MsolDomainAuthentication -DomainName $domainName -FederationBrandName $domainName -Authentication Federated -PassiveLogOnUri $passiveLogOnUri -ActiveLogOnUri $activeLogonUri -SigningCertificate $signingcertificate -IssuerUri $issuerUri -LogOffUri $logOffUri -PreferredAuthenticationProtocol "SAMLP"

Create Dynamic Group for all licensed Users

```
(user.userType -eq "member") and (user.department -ne "NotSupport") and (user.accountEnabled -eq true) and (user.assignedPlans -any (assignedPlan.servicePlanId -ne "" -and assignedPlan.capabilityStatus -eq "Enabled"))
```

this requires that the user type is set to "member."

That can be removed.

Creating a Secure Site-to-Site VPN Connection in Azure: A Step-by-Step Guide

https://medium.com/@subhampradhan966/creating-a-secure-site-to-site-vpn-connection-in-azure-a-step-by-step-guide-b4689f7cbb35

Here are the key features used in this implementation:

Virtual Network (VNet):

- VNets in Azure provide the foundation for hosting VMs and other Azure resources. They serve as isolated networks within Azure and are essential for establishing connectivity between on-premises and Azure environments.

Virtual Network Gateway:

- The Virtual Network Gateway serves as the Azure endpoint of the VPN tunnel. It provides the necessary infrastructure to establish and manage the VPN connection between Azure and the on-premises VPN device.

Local Network Gateway:

- The Local Network Gateway represents the on-premises VPN device in Azure. It defines the IP address, address space, and other parameters required to establish a secure connection between the on-premises network and Azure VNet.

VPN Gateway SKUs:

- Azure offers different VPN Gateway SKUs with varying performance and throughput capabilities. Choosing the appropriate SKU depends on factors such as the volume of traffic, latency requirements, and budget considerations.

Connection Types:

- Azure supports different connection types for VPN gateways, including Site-to-Site (IPsec), Point-to-Site (SSL VPN), and ExpressRoute. For site-to-site VPN connections, the IPsec protocol is commonly used for its robust security and compatibility with various VPN devices.

Pre-shared Keys (PSK):

- Pre-shared keys are used for authentication between the Azure VPN gateway and the on-premises VPN device. These keys ensure that only authorized parties can establish the VPN tunnel and communicate securely.

Configuration File:

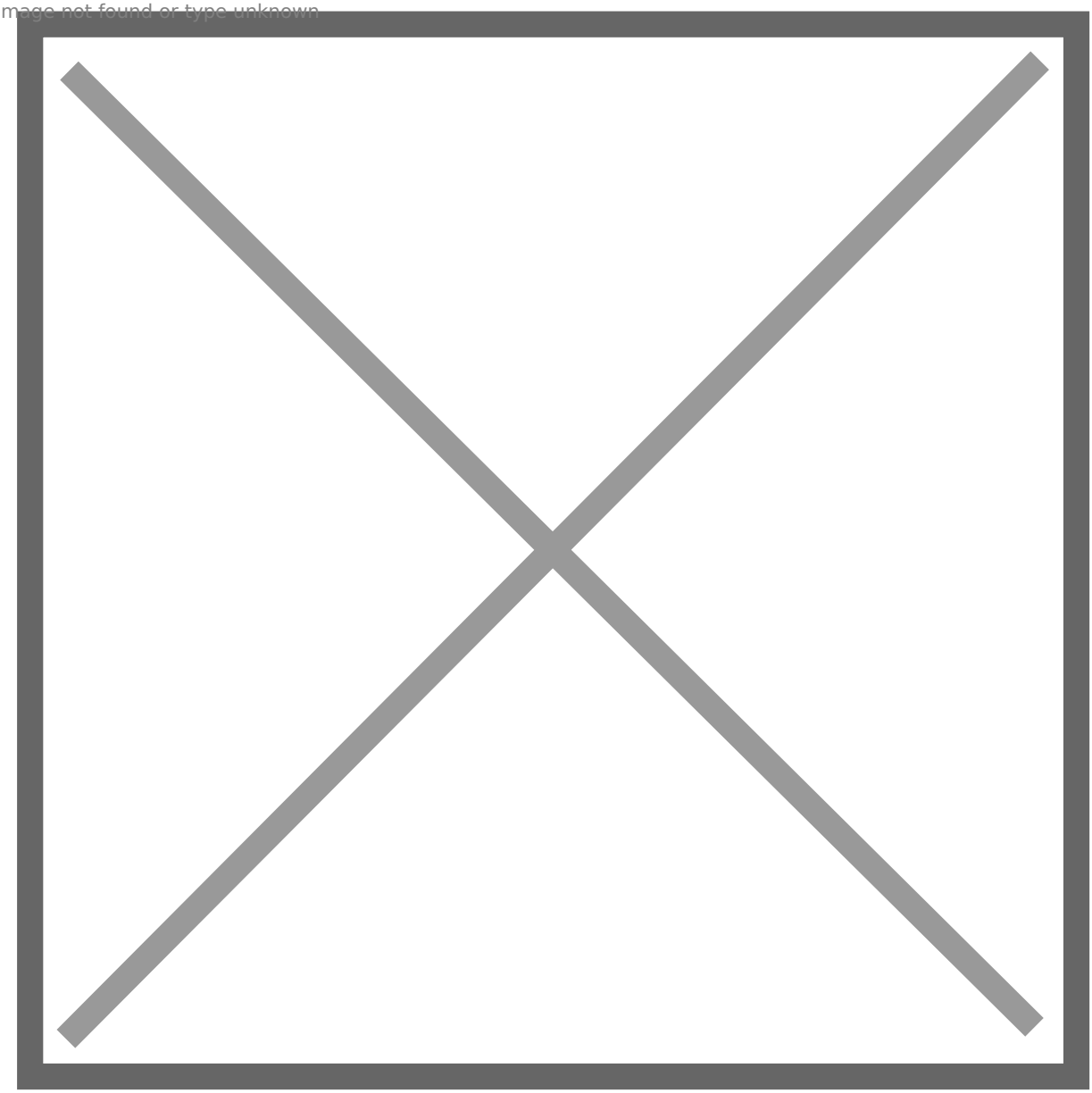
- Azure generates a configuration file containing the necessary settings and parameters for configuring the on-premises VPN device. This file includes details such as the VPN gateway IP address, pre-shared key, encryption protocols, and other configuration options.

Dynamic Routing:

- Azure VPN gateways support dynamic routing protocols such as BGP (Border Gateway Protocol), which enable automatic route propagation between on-premises and Azure networks. Dynamic routing enhances flexibility and scalability in complex network environments.

Step-by-Step Implementation:

Image not found or type unknown



Azure Site-to-Site VPN Connection Architecture

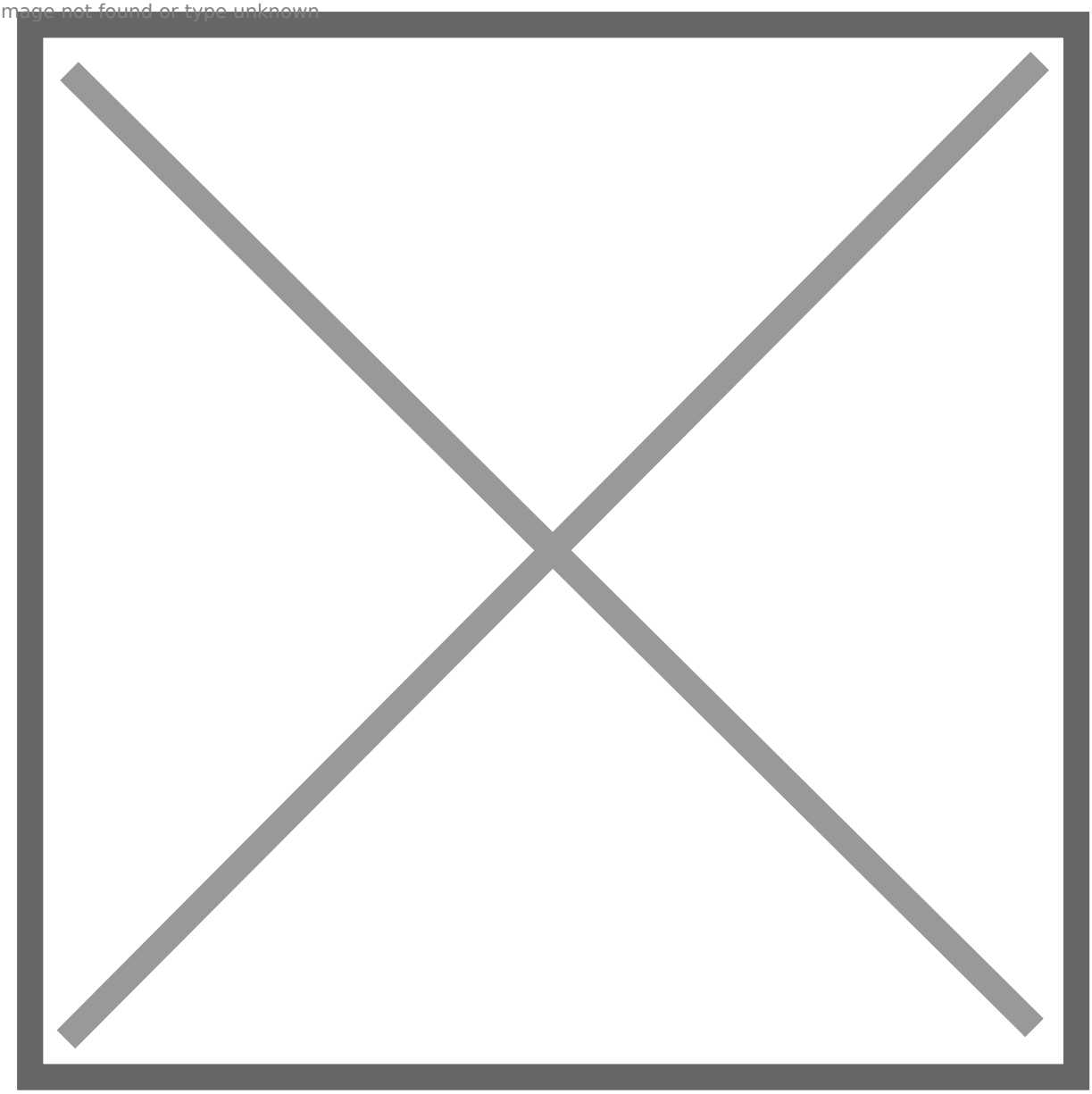
Step 1: Create a Subscription

1. Go to the Azure portal (portal.azure.com).
2. Navigate to “Subscriptions”.
3. Click on “Add” to create a new subscription if you don’t have one already.

Step 2: Create a Resource

1. In the Azure portal, navigate to “Resource groups”.
2. Click on “Create”.
3. Provide a name for your resource group.
4. Choose the subscription you created earlier.
5. Select a region for your resource group.
6. Click on “Review + create” and then “Create” to finalize the creation of the resource group.

Image not found or type unknown

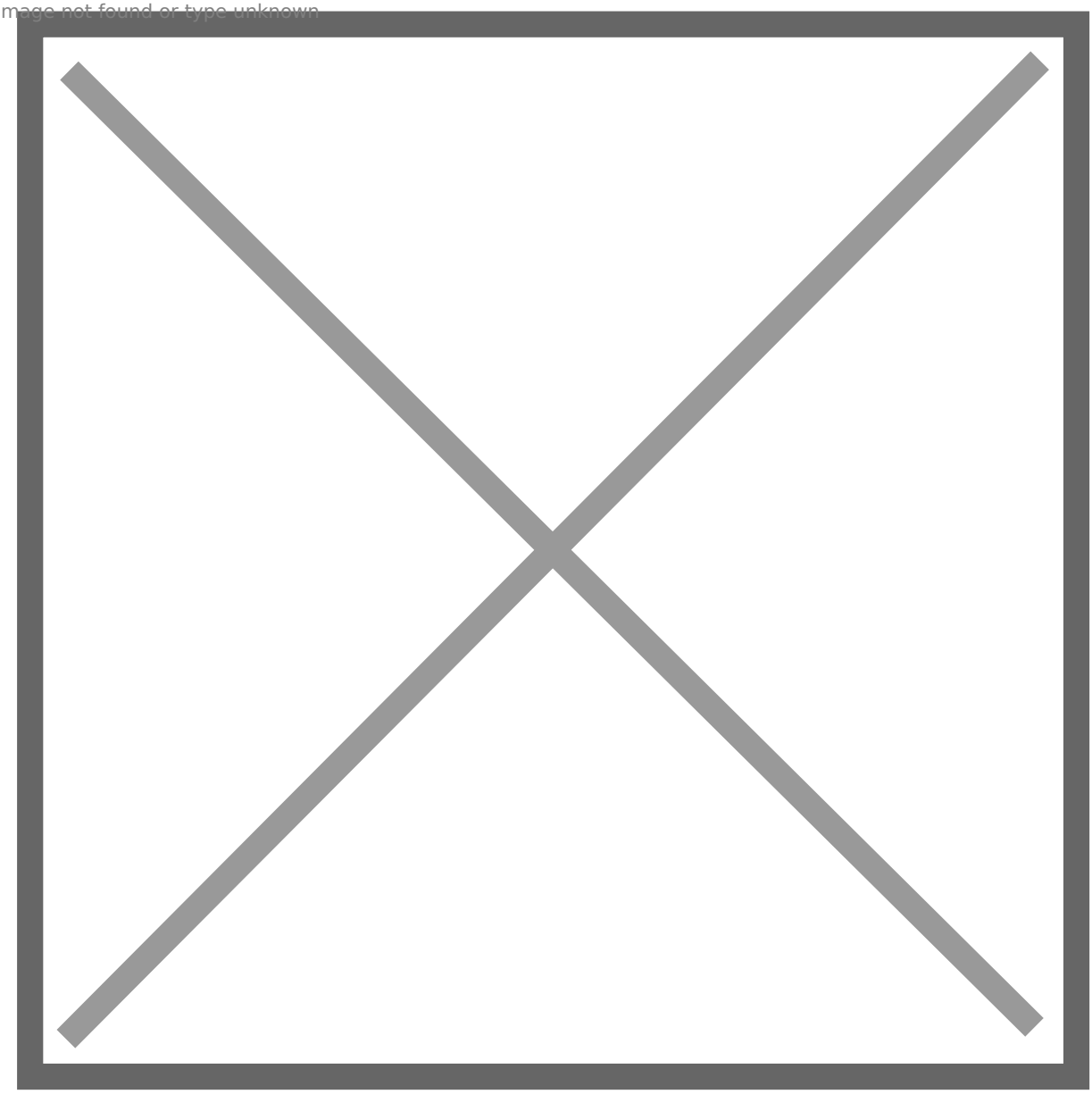


Step 3: Create a Virtual Network

1. In the Azure portal, navigate to “Virtual networks”.
2. Click on “Add” to create a new virtual network.
3. Fill out the required details:

- Name: Provide a name for your virtual network.
- Address space: Define the address space for your virtual network.
- Subnet: Add a subnet and define its address range.
- Subscription: Choose your subscription.
- Resource group: Select the resource group created earlier.
- Location: Choose the location for your virtual network.
- Click on “Review + create” and then “Create” to create the virtual network.

Image not found or type unknown



Create 2 subnets :

S2S-SUBNET-1 : 10.0.1.0/24

S2S-SUBNET-2 : **10.0.2.0/24**

Image not found or type unknown

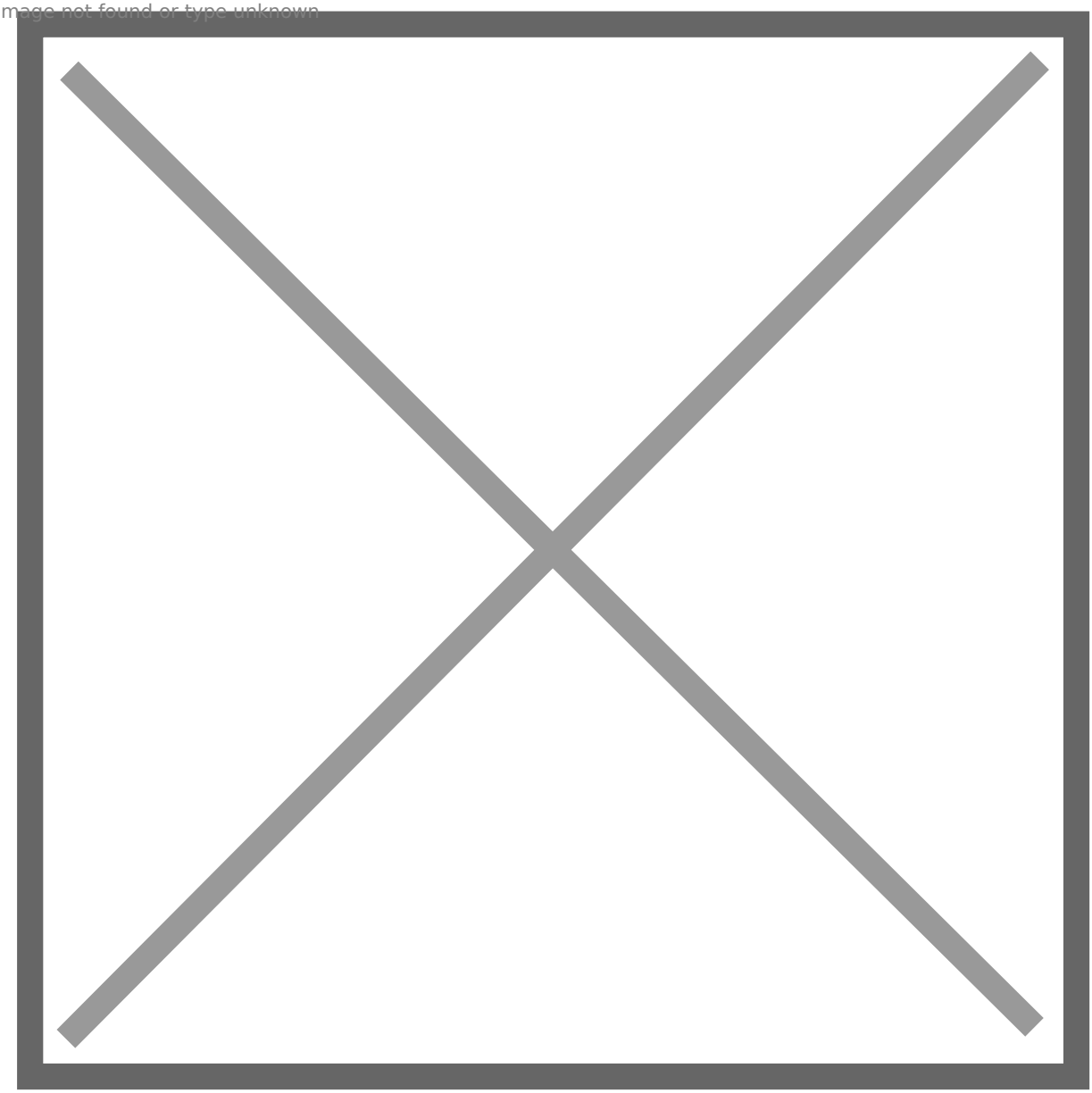


Image not found or type unknown

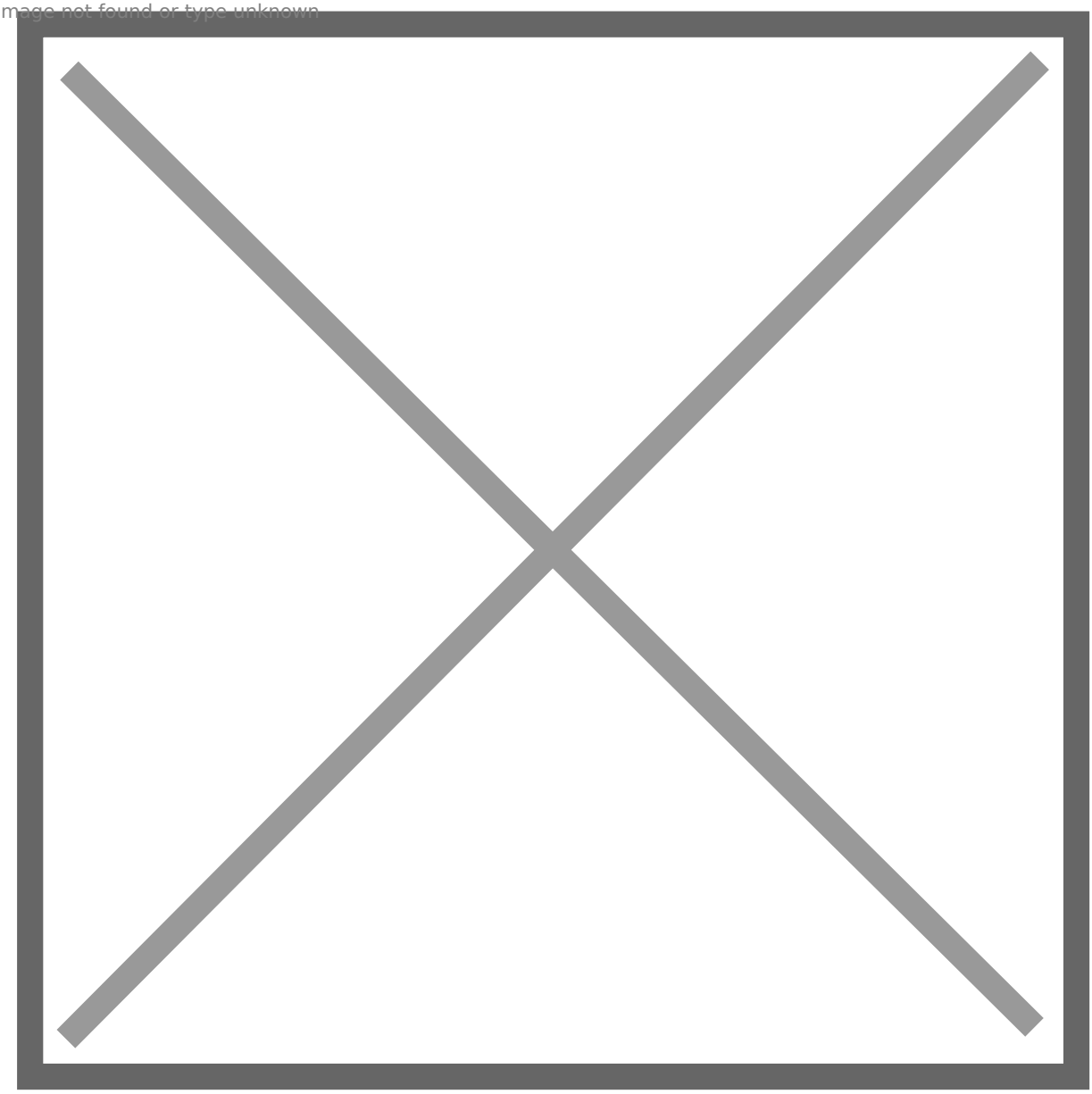


Image not found or type unknown

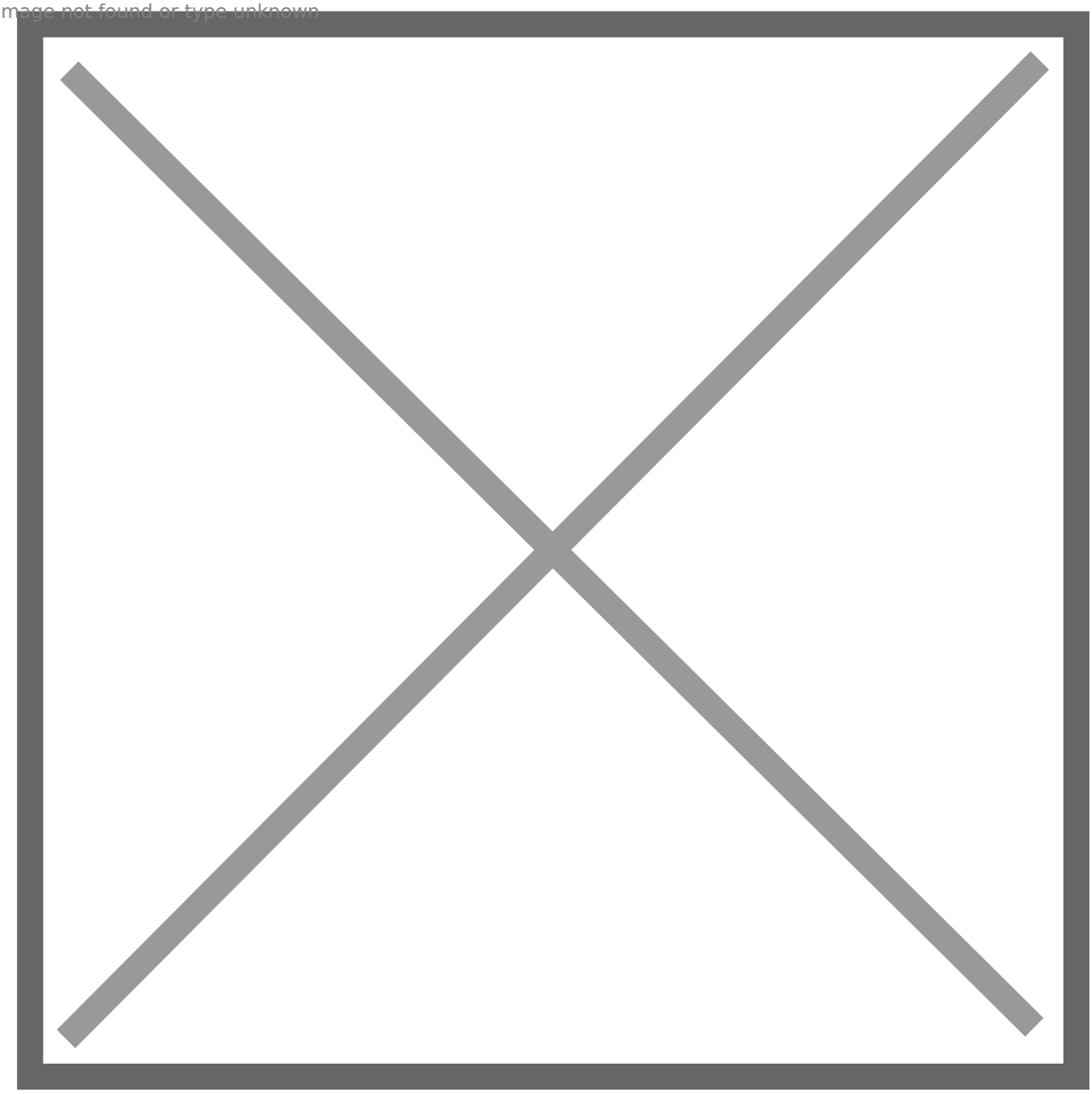
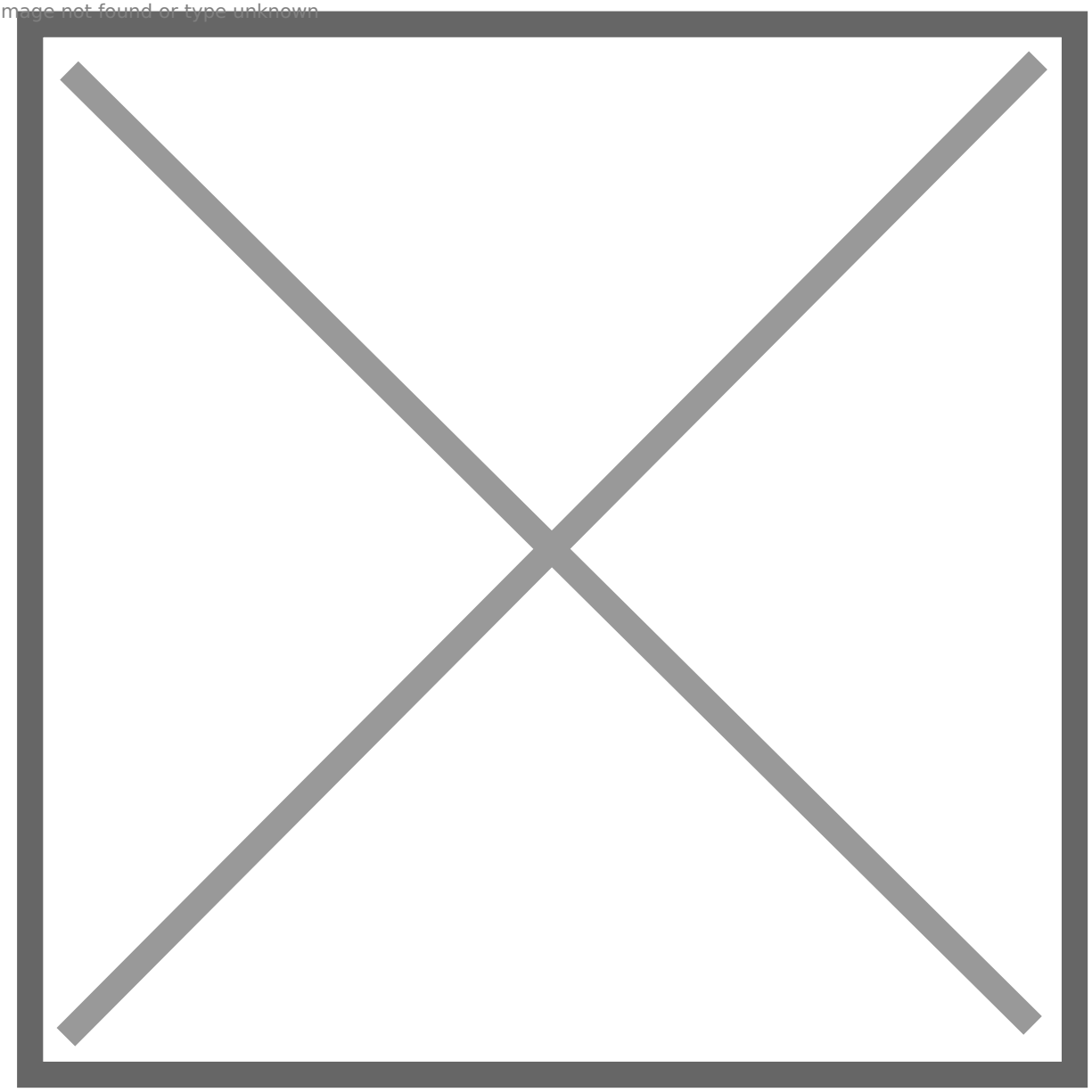


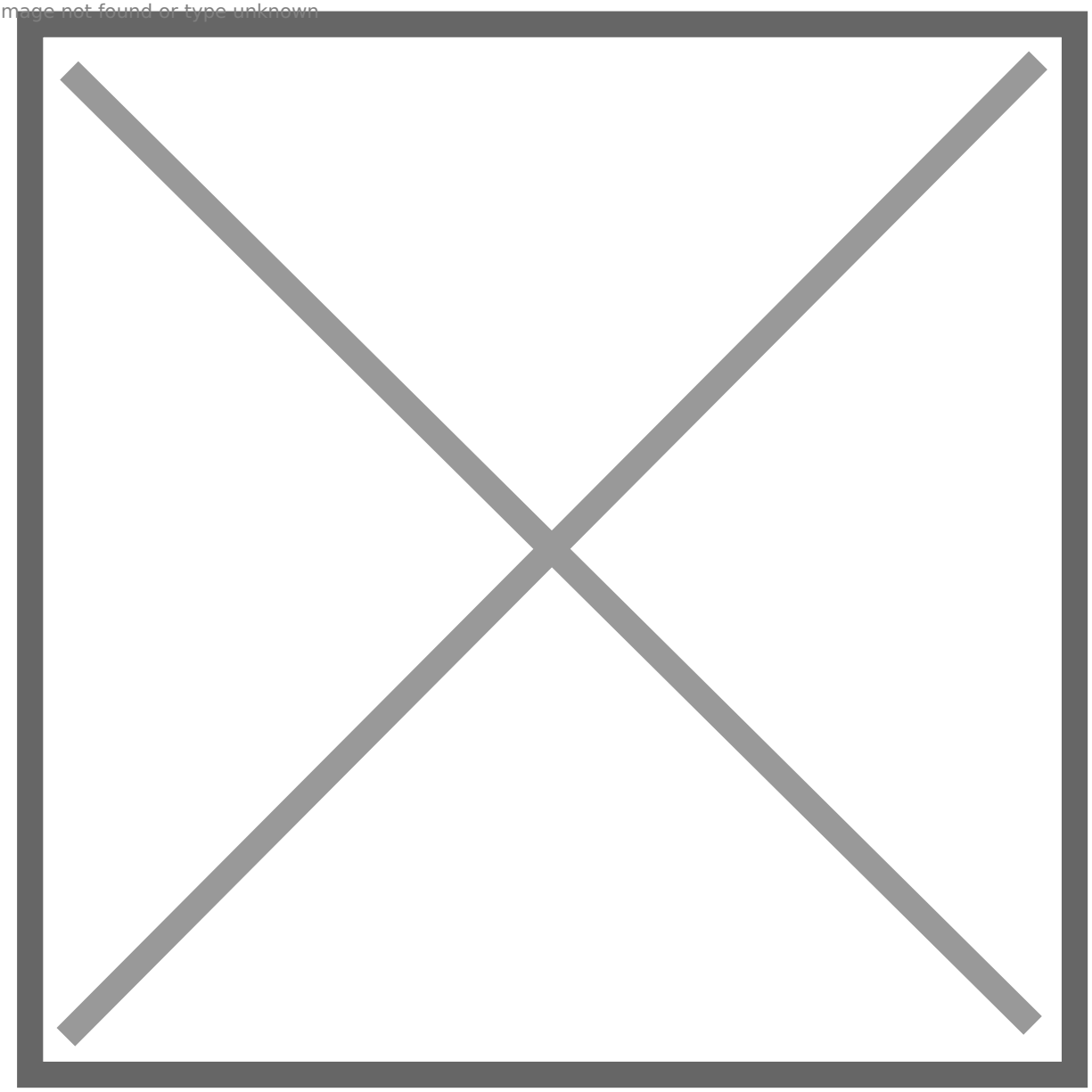
Image not found or type unknown



Add Gateway Subnet

1. After creating the virtual network, navigate to its settings.
2. Click on “Subnets”.
3. Click on “+ Gateway subnet” to add a gateway subnet.
4. Name your subnet (e.g., “GatewaySubnet”).
5. Define the address range for the subnet. Note: It should be a valid CIDR block within the address space of your virtual network.
6. Click on “OK” to create the gateway subnet.

Image not found or type unknown



Step 4: Create a Virtual Network Gateway

1. Go to “Virtual network gateways” in the Azure portal.
2. Click on “Add” to create a new virtual network gateway.
3. Provide the necessary details such as gateway type, VPN type, SKU, and virtual network settings.
4. Select the same resource group created in Step 2.

5. Wait for the deployment to complete.

Image not found or type unknown

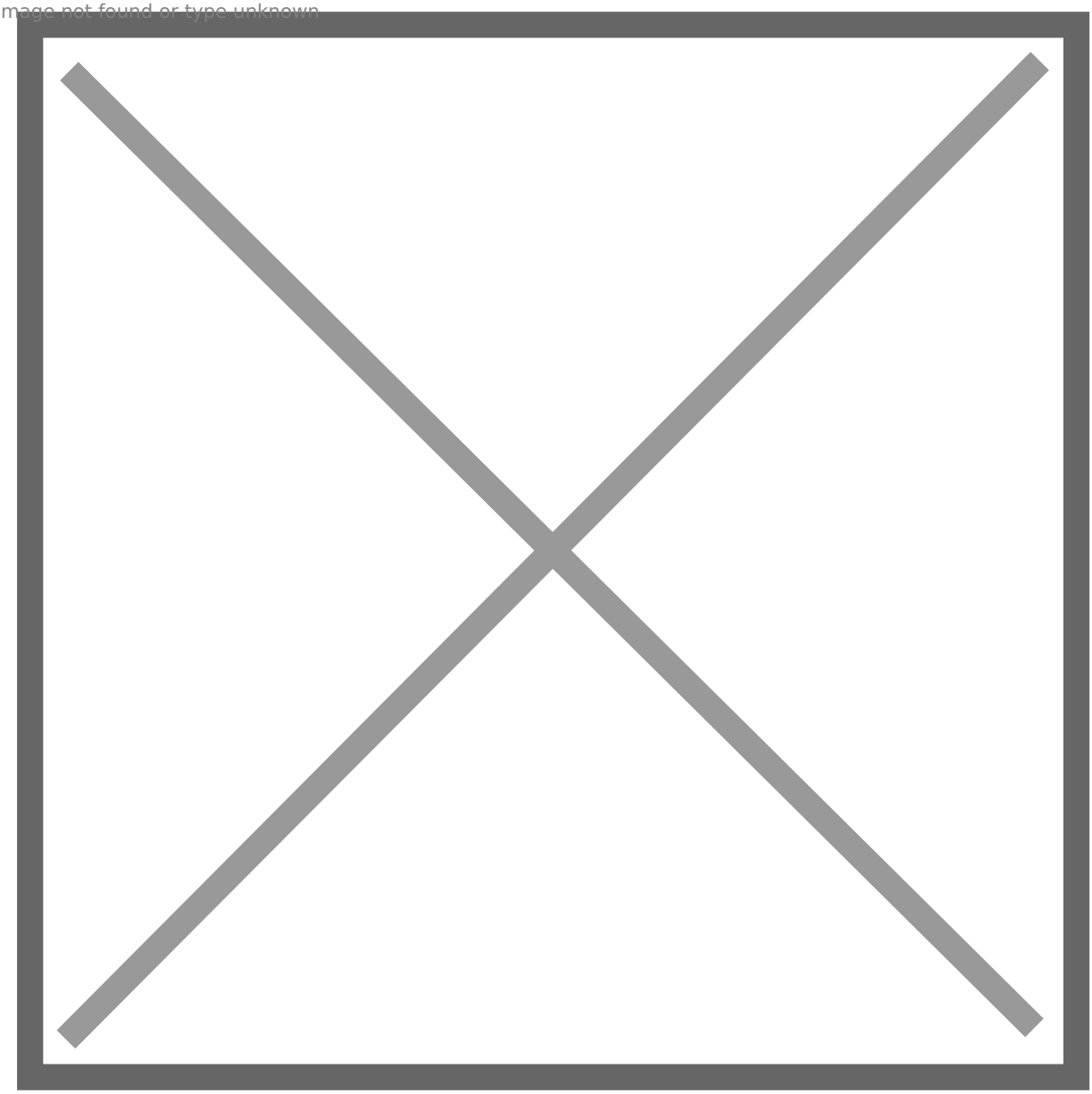
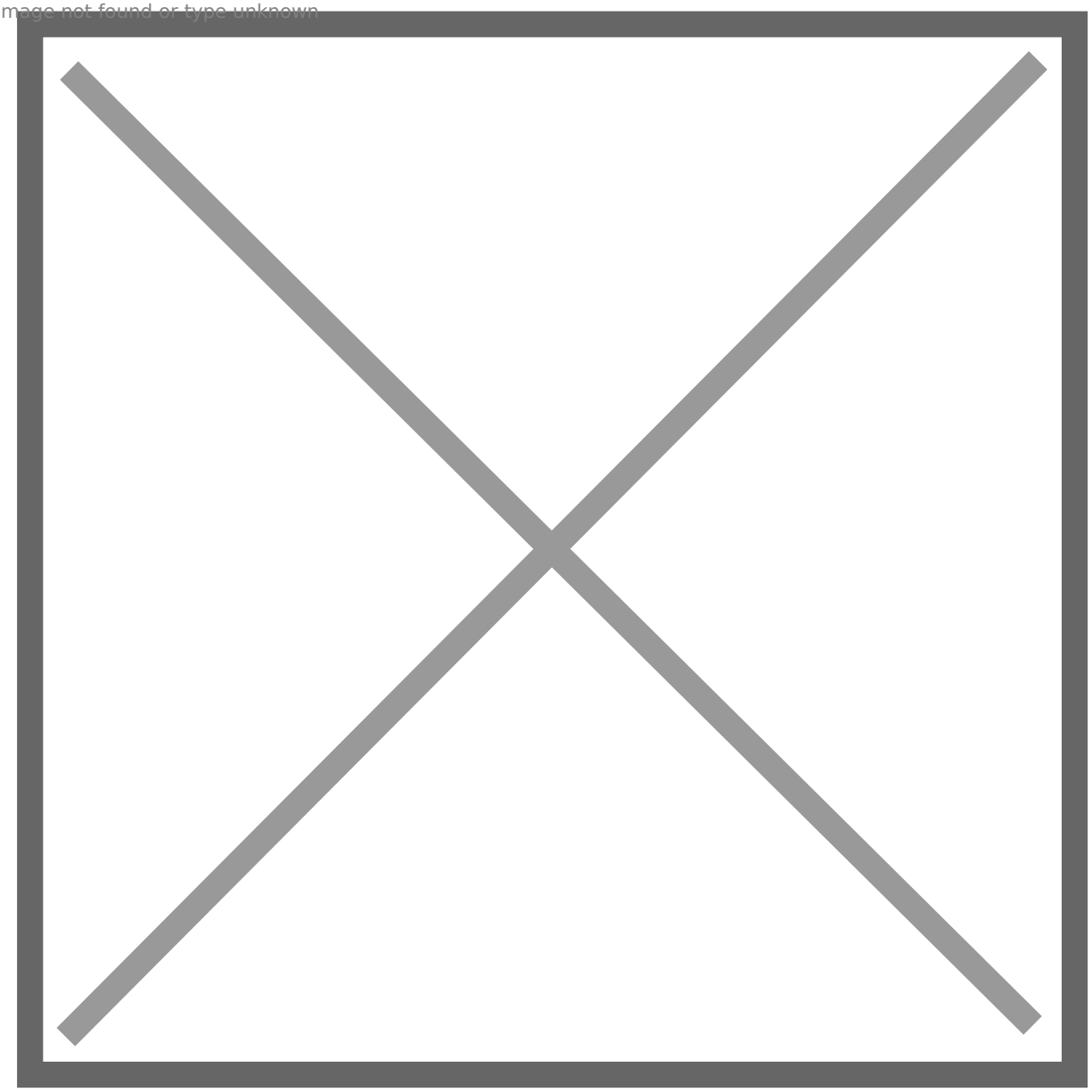
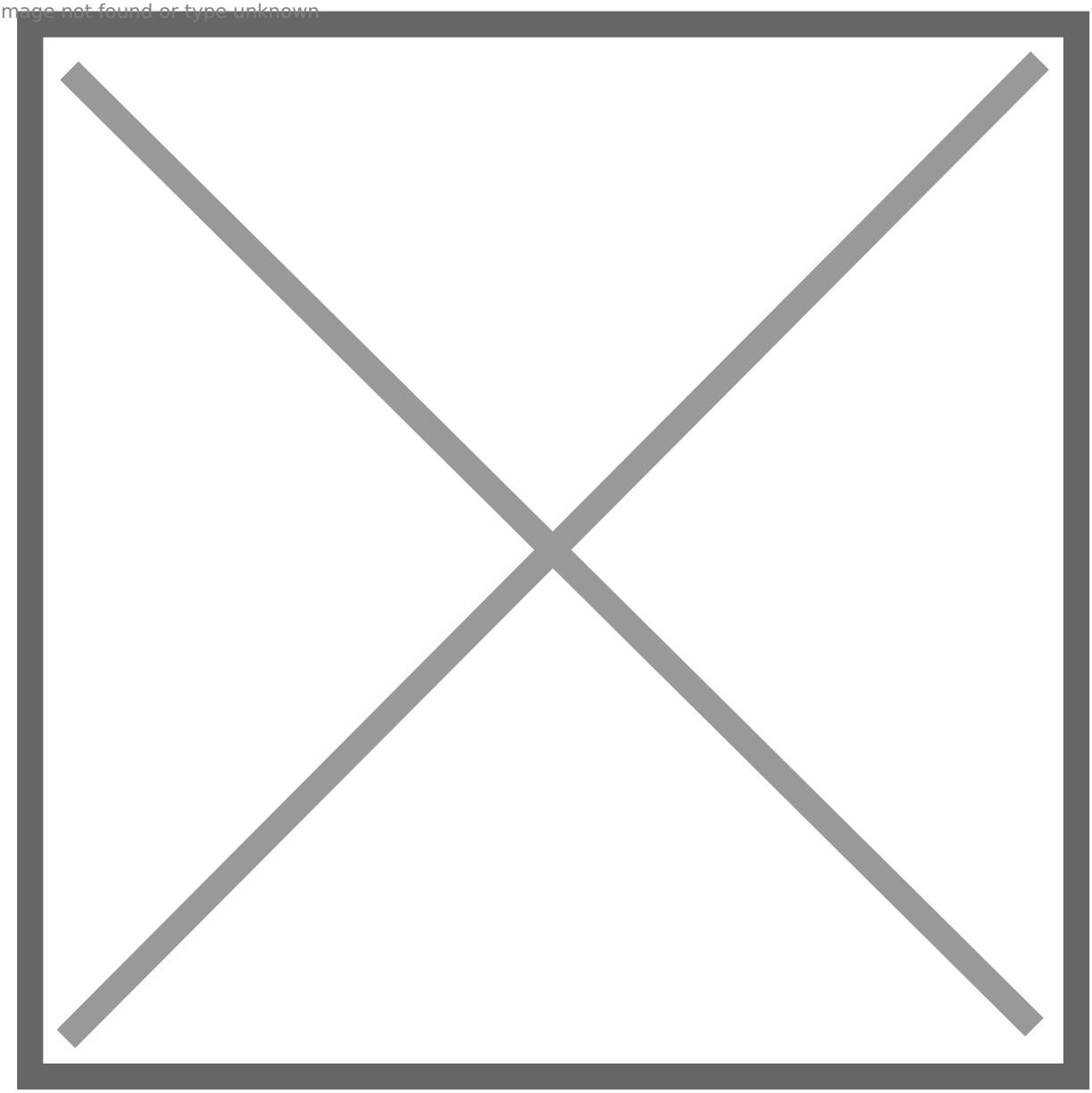


Image not found or type unknown



For Creating Virtual Network Gateway, it will take more than **25 minutes** ;

Image not found or type unknown

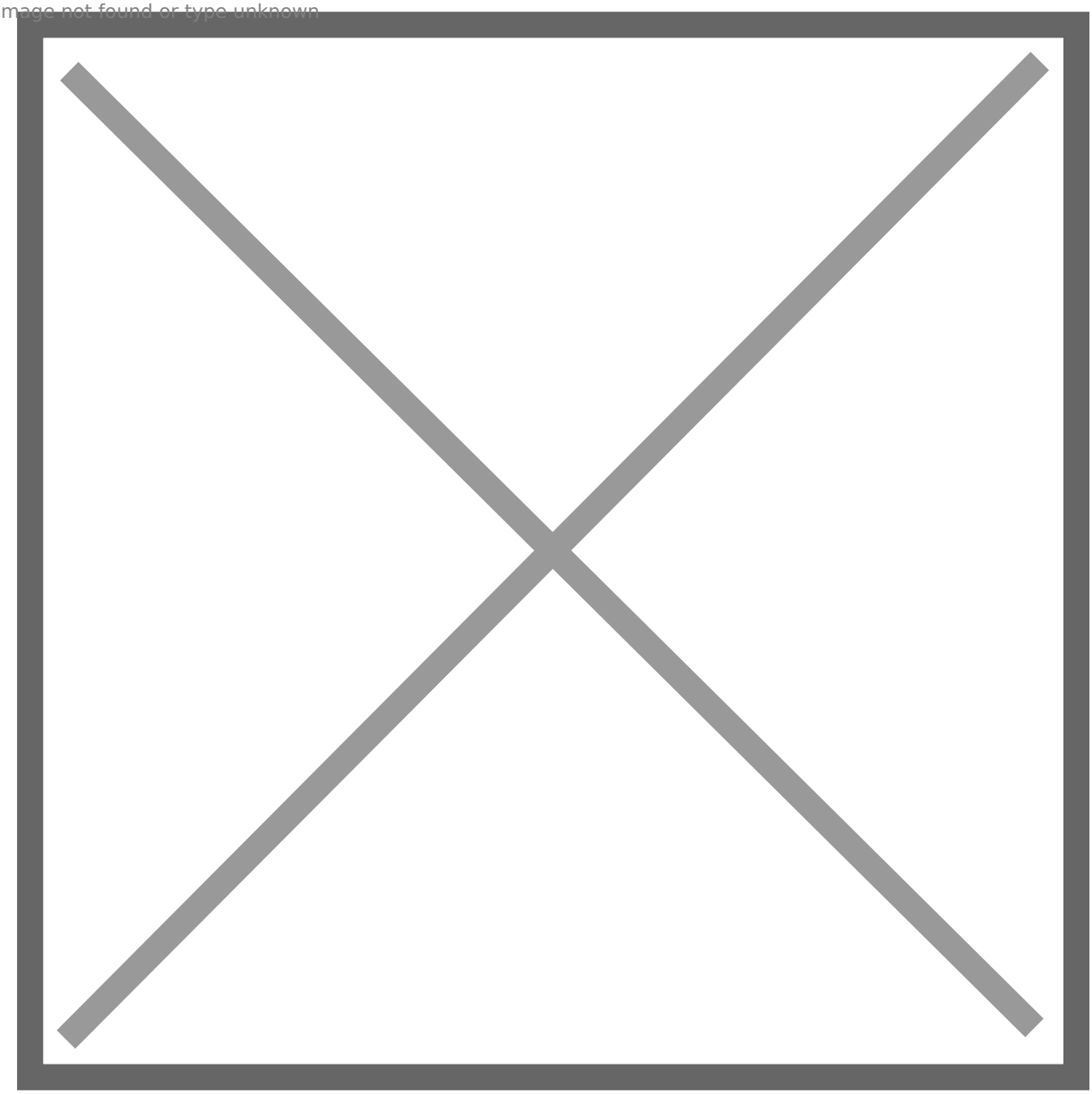


Step 5: Create a Local Network Gateway

1. In the Azure portal, go to “Local network gateways”.
2. Click on “Add” to create a new local network gateway.
3. Enter the required information, including name, IP address of the local VPN device, and the address space.

4. Associate the local network gateway with the same resource group as before.
5. Complete the creation process.

Image not found or type unknown



If static : Need IP from Client

If Dynamic : Need Domain from Client

Image not found or type unknown

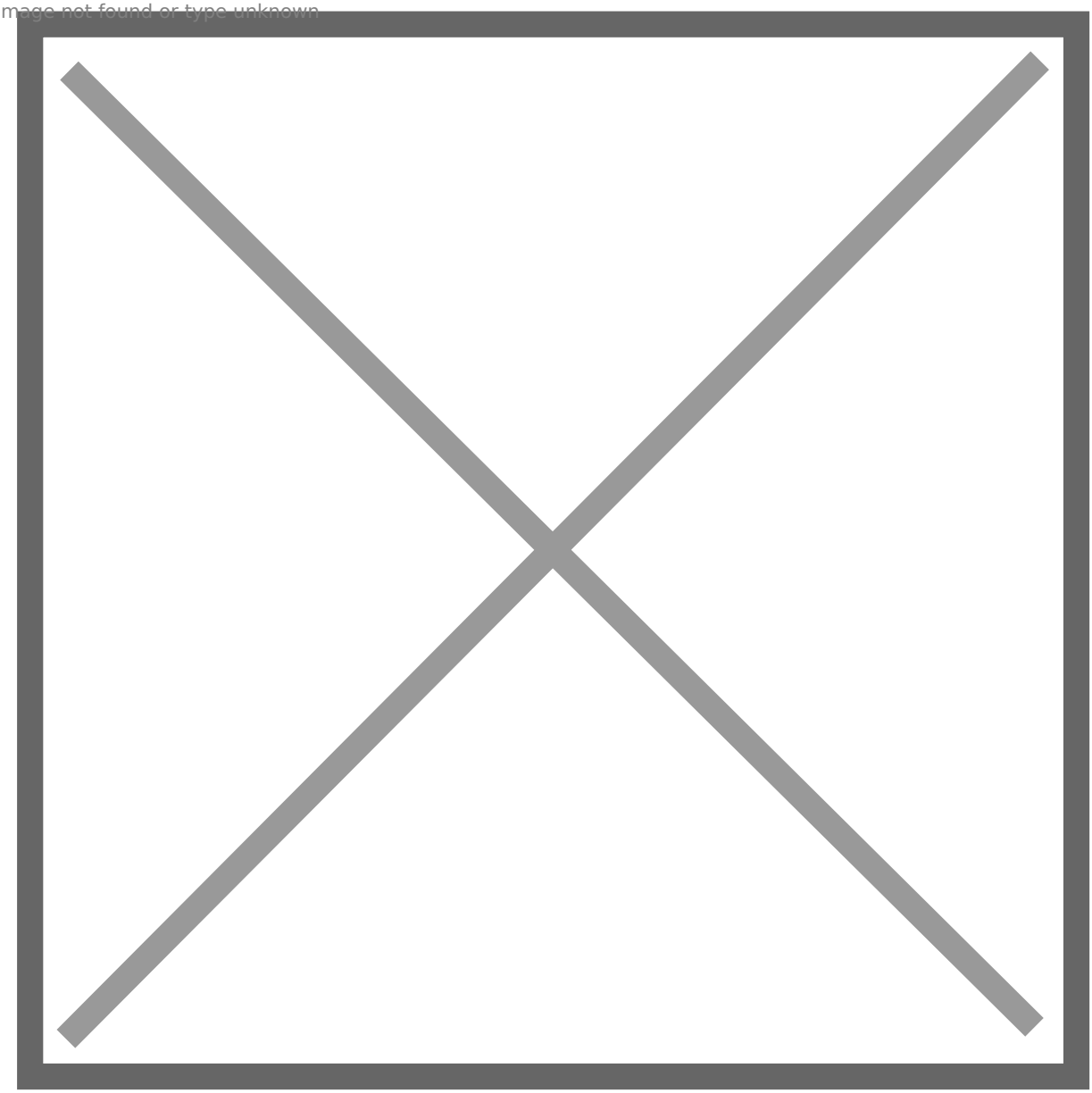
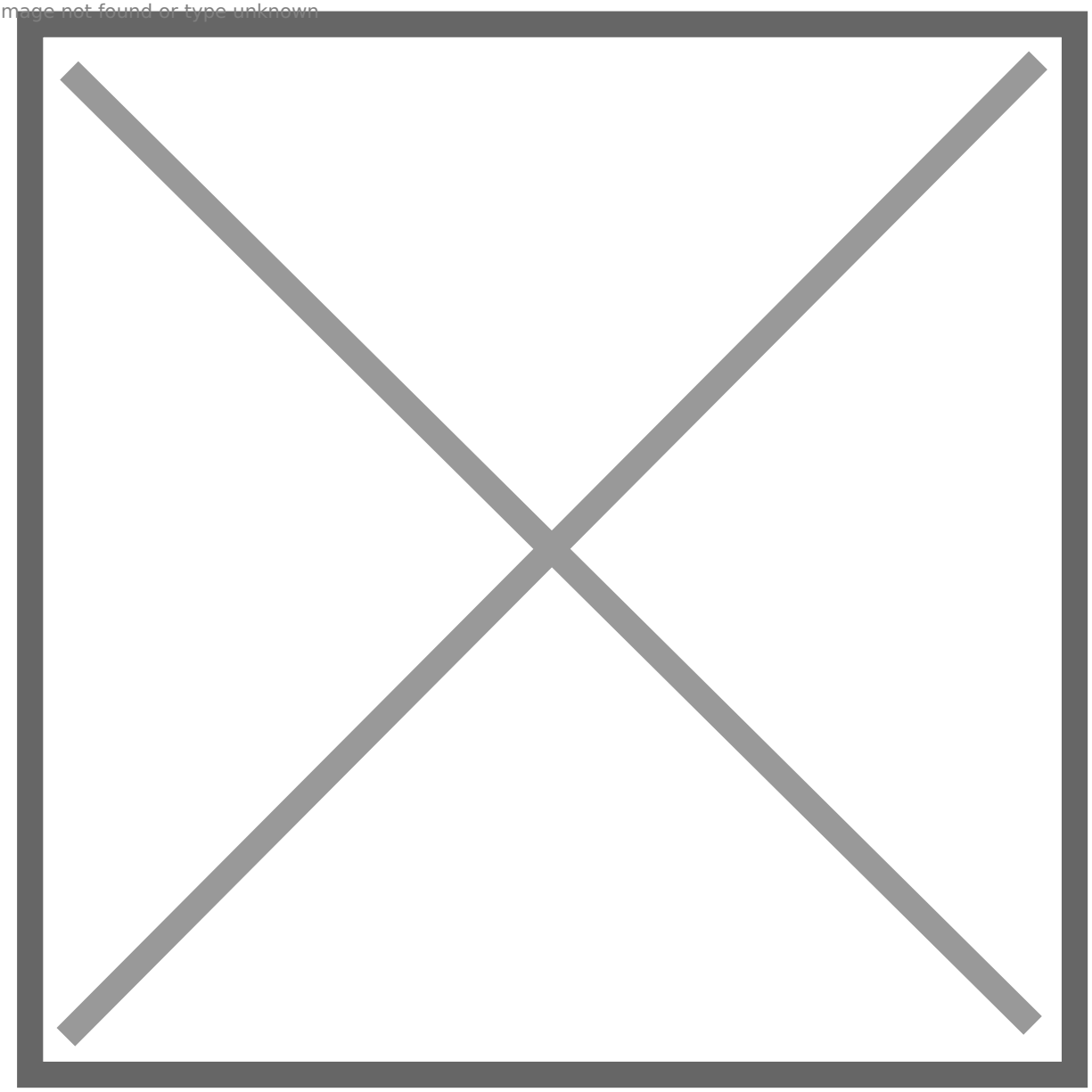


Image not found or type unknown



Step 6: Add Connection — Virtual Network Gateway

1. Navigate to the virtual network gateway resource created in Step 4.
2. Select “Connections” and then click on “Add”.
3. Choose the virtual network gateway and local network gateway that you created earlier.
4. Configure the connection type as “Site-to-Site (IPsec)”.

5. Provide the pre-shared key, IP address (static or dynamic), and choose the vendor (generic/cisco).
6. Download the configuration file for the VPN device. If using a dynamic IP address, ensure you have a domain name associated with it.

Image not found or type unknown

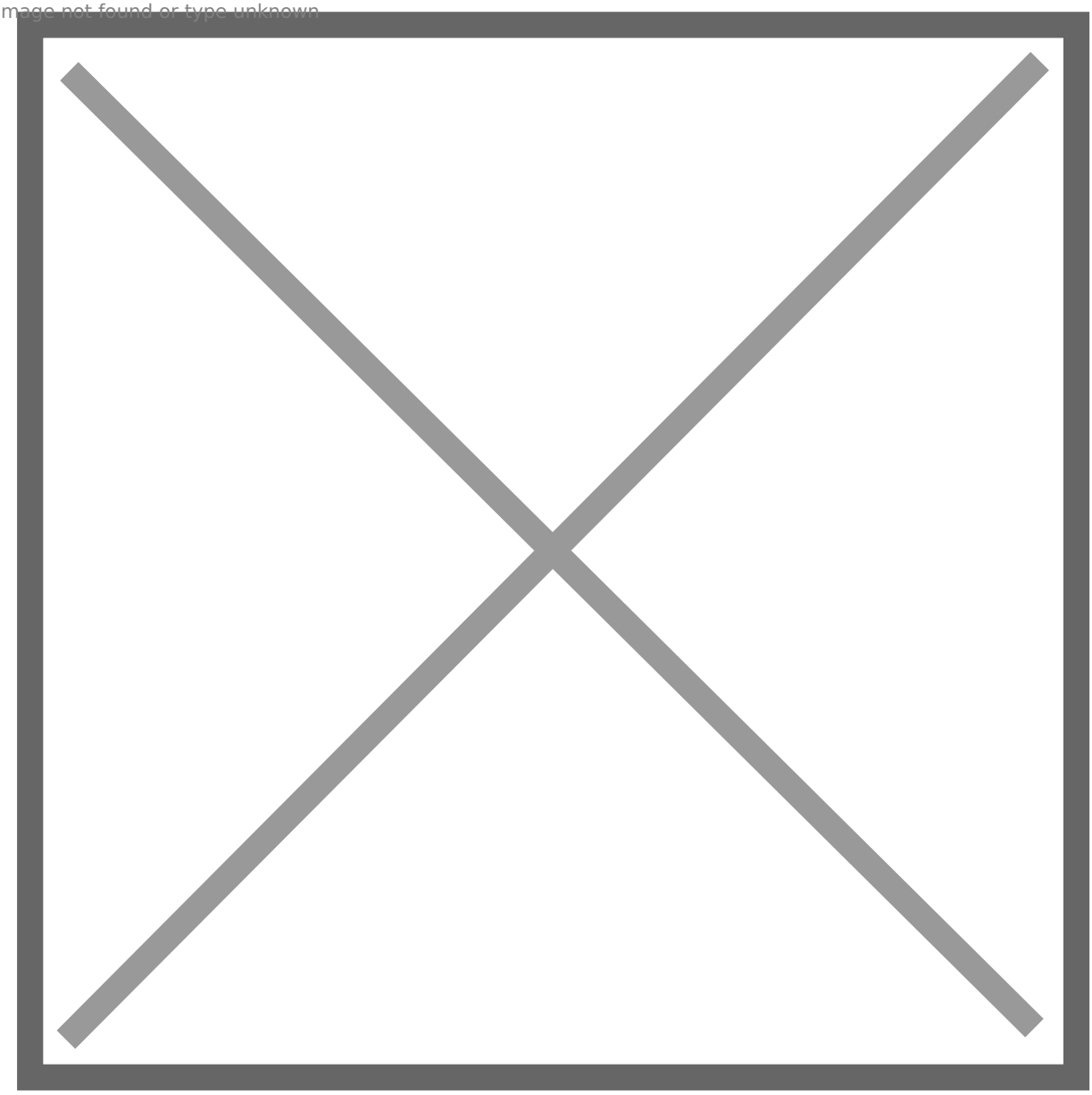


Image not found or type unknown

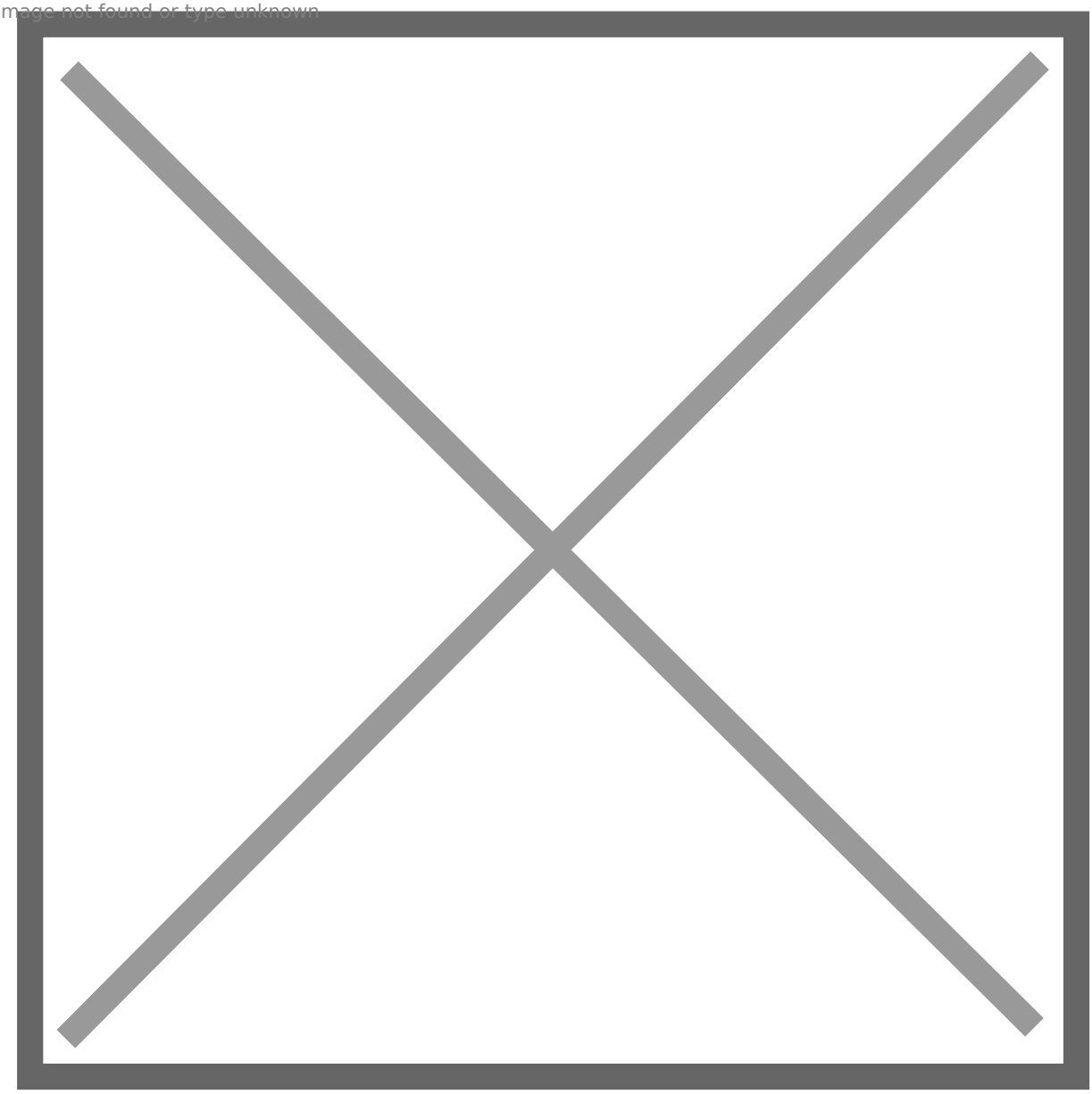


Image not found or type unknown

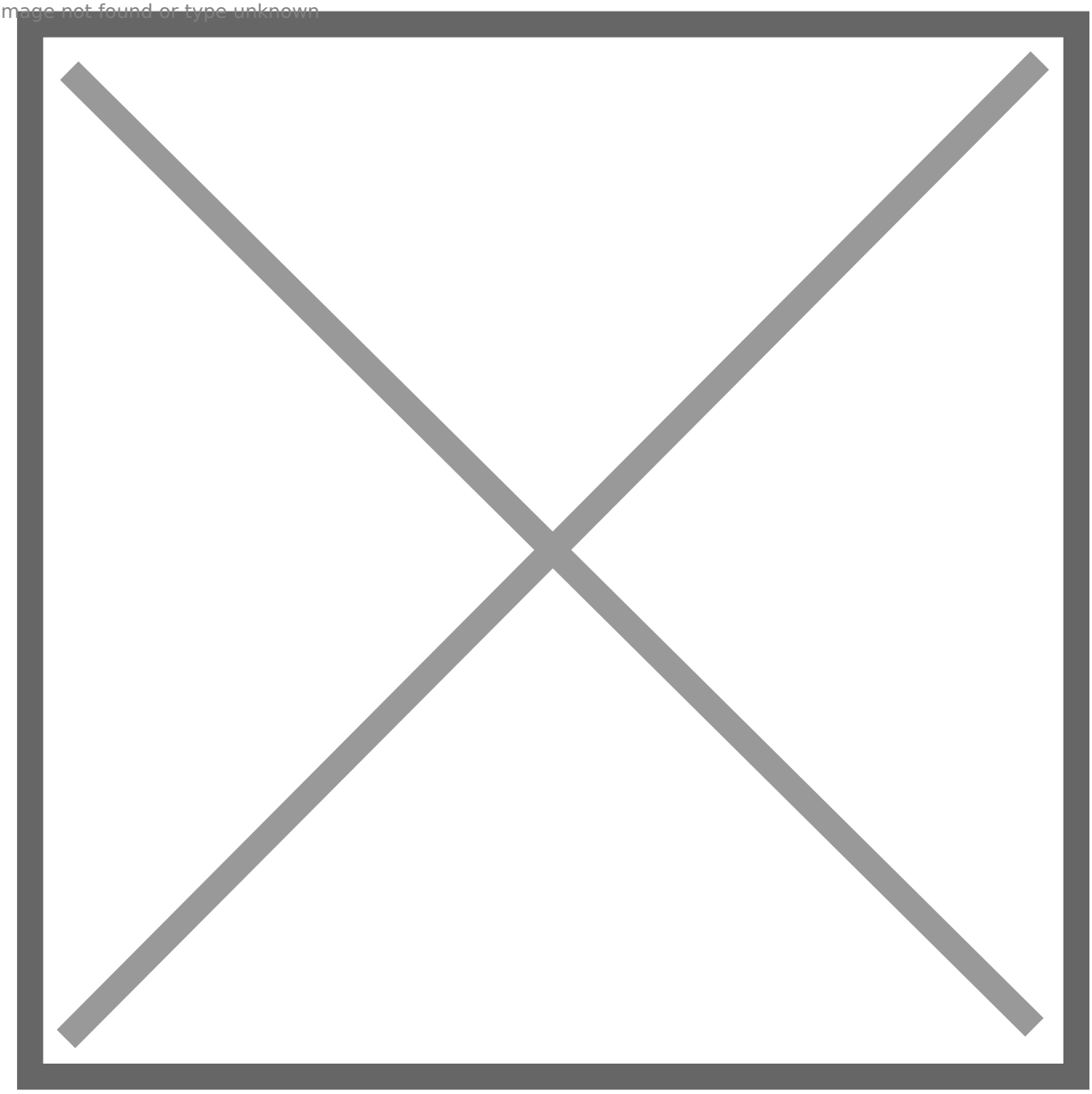


Image not found or type unknown

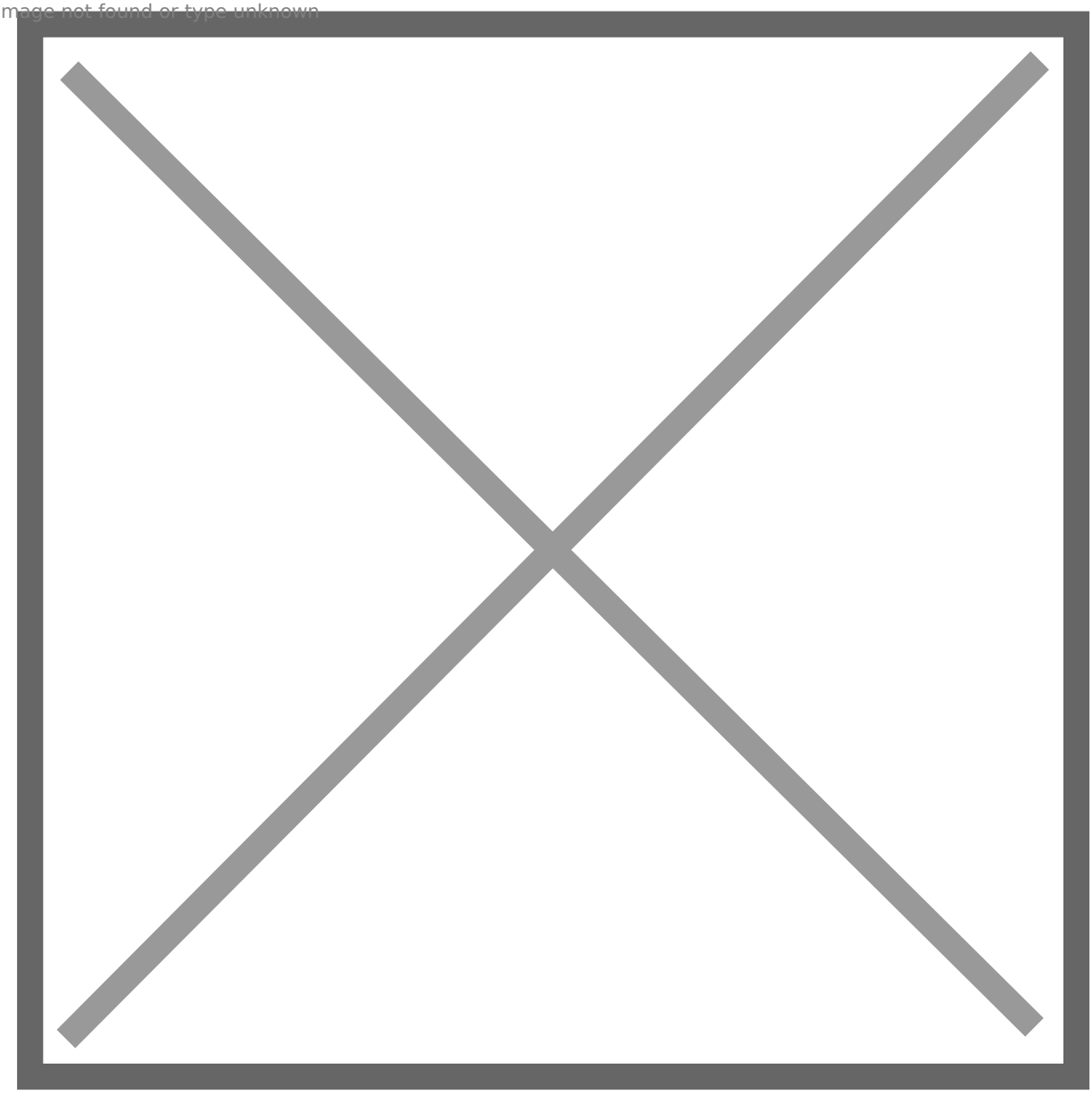


Image not found or type unknown

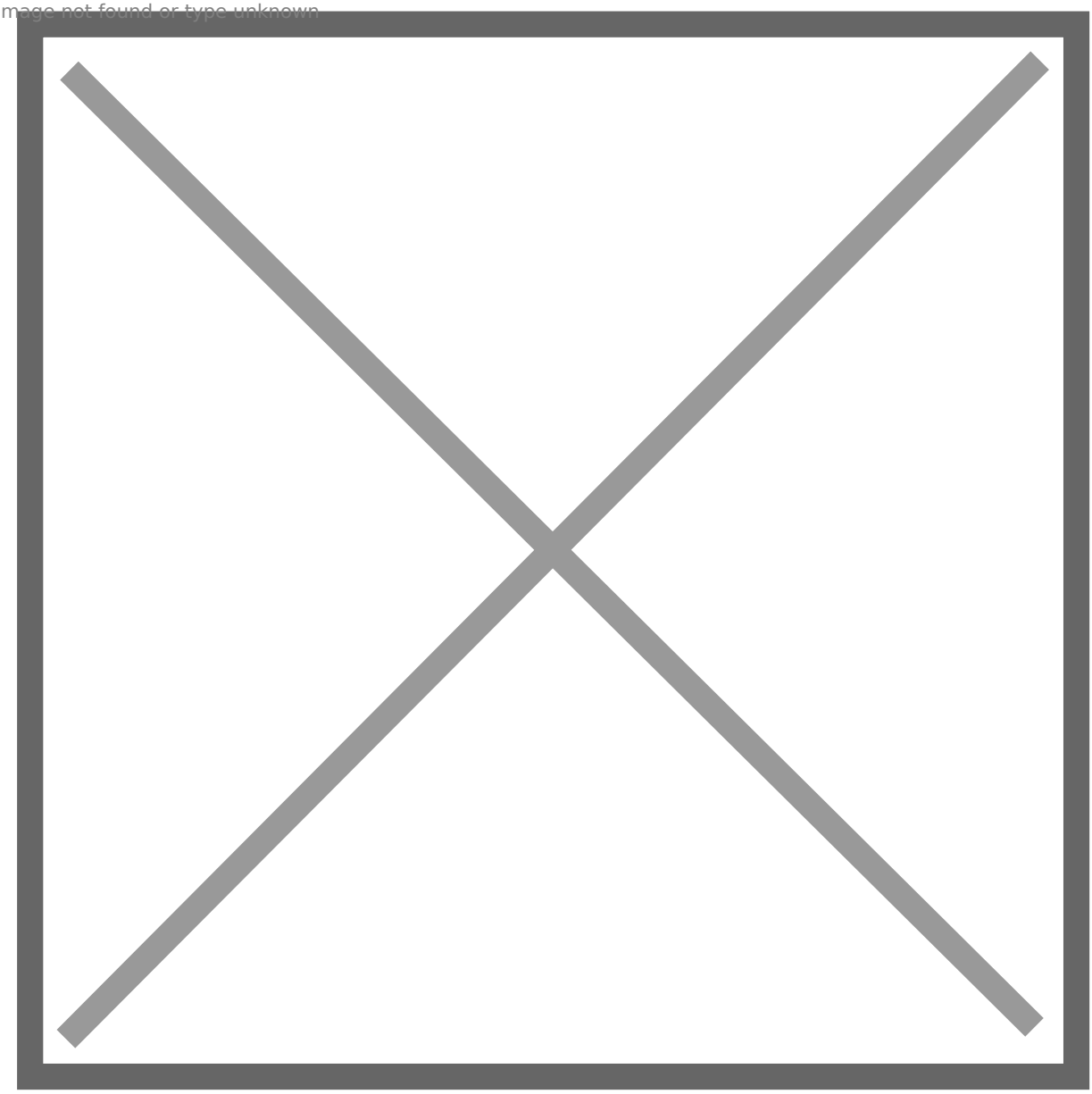
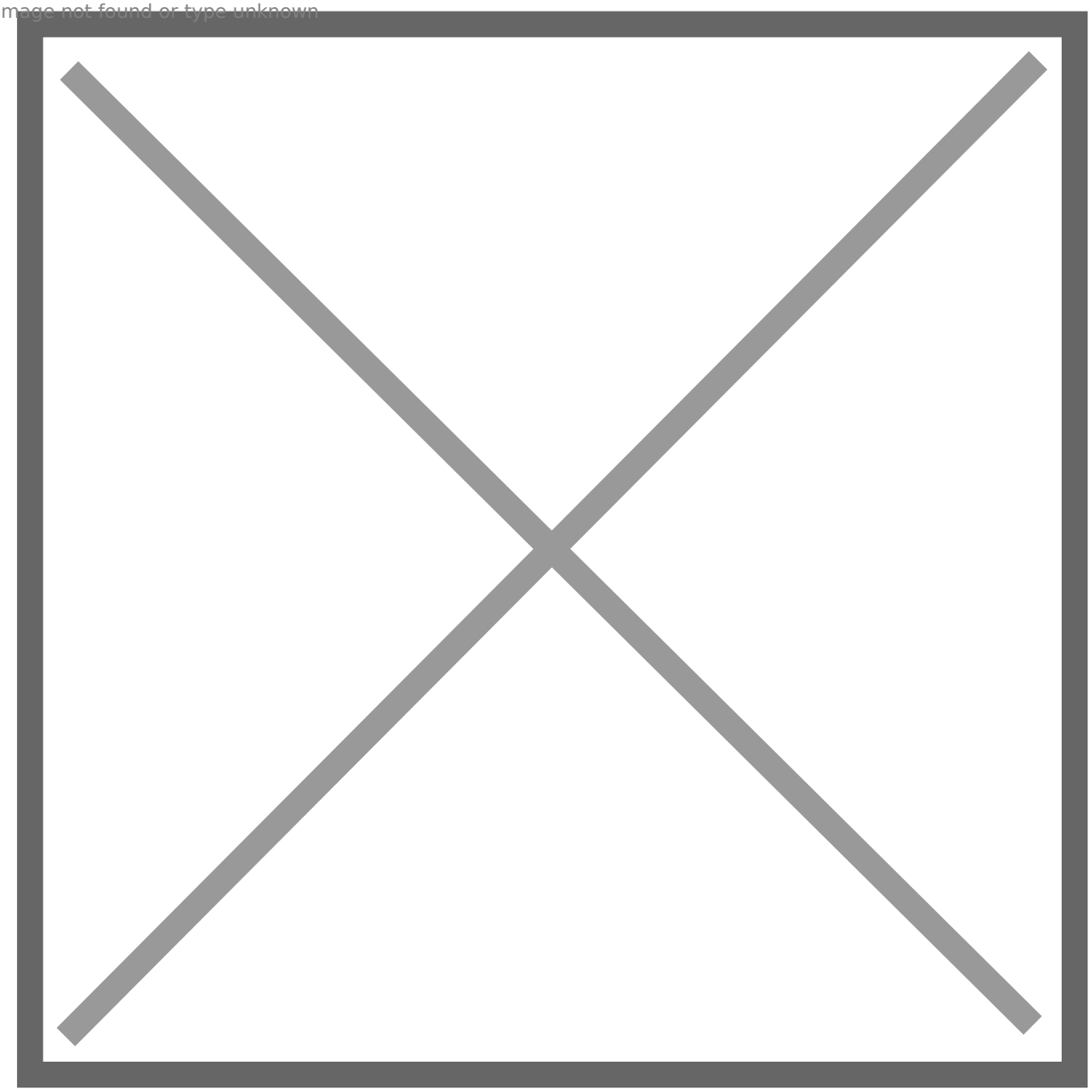


Image not found or type unknown



Step 7: Configure Client’s VPN Device

1. Share the downloaded configuration file with your client.
2. Instruct your client to configure their VPN device (Cisco or generic) using the details provided in the configuration file.
3. If the IP address is dynamic, ensure they use the domain name for setup.

Image not found or type unknown

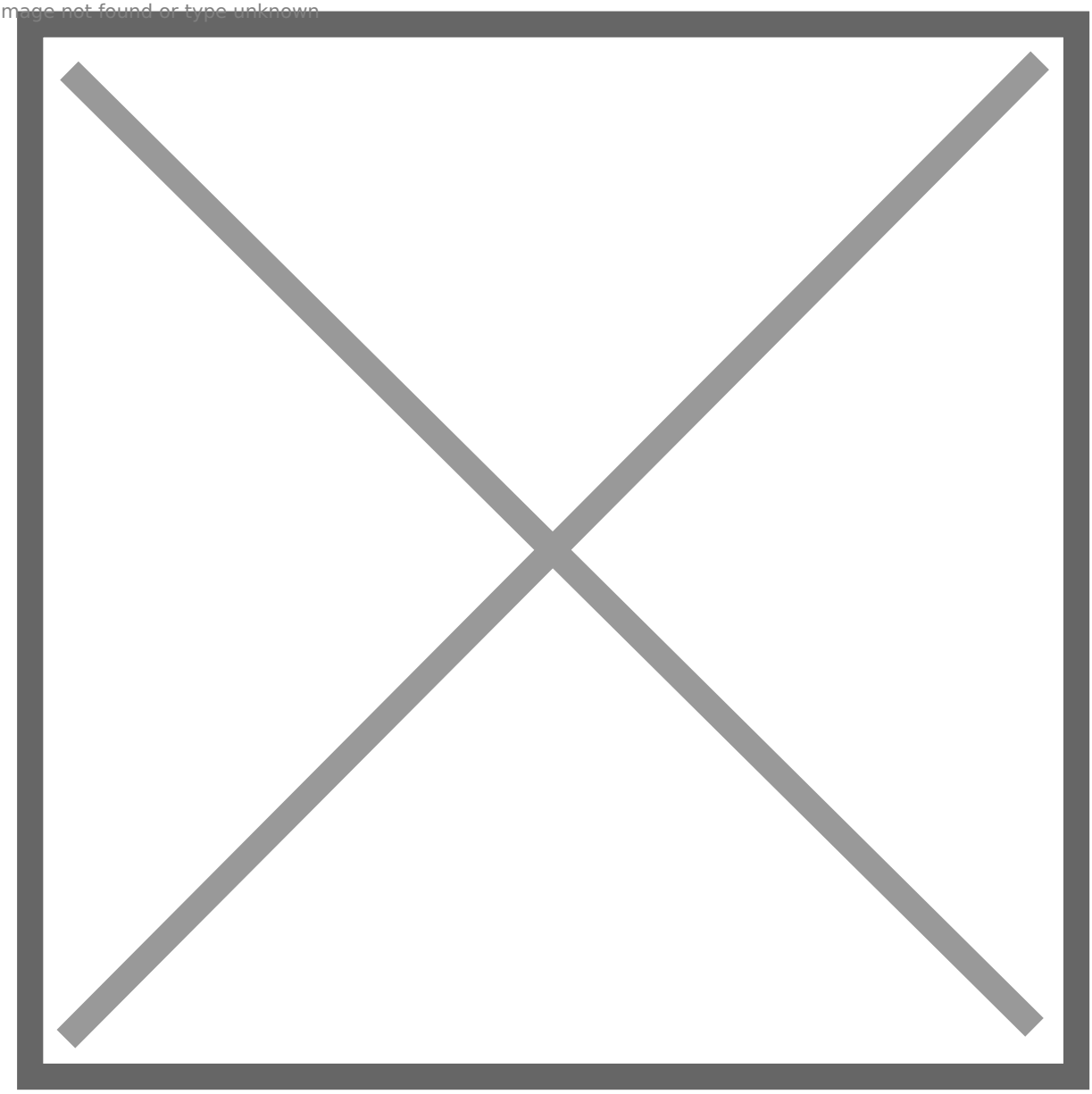


Image not found or type unknown

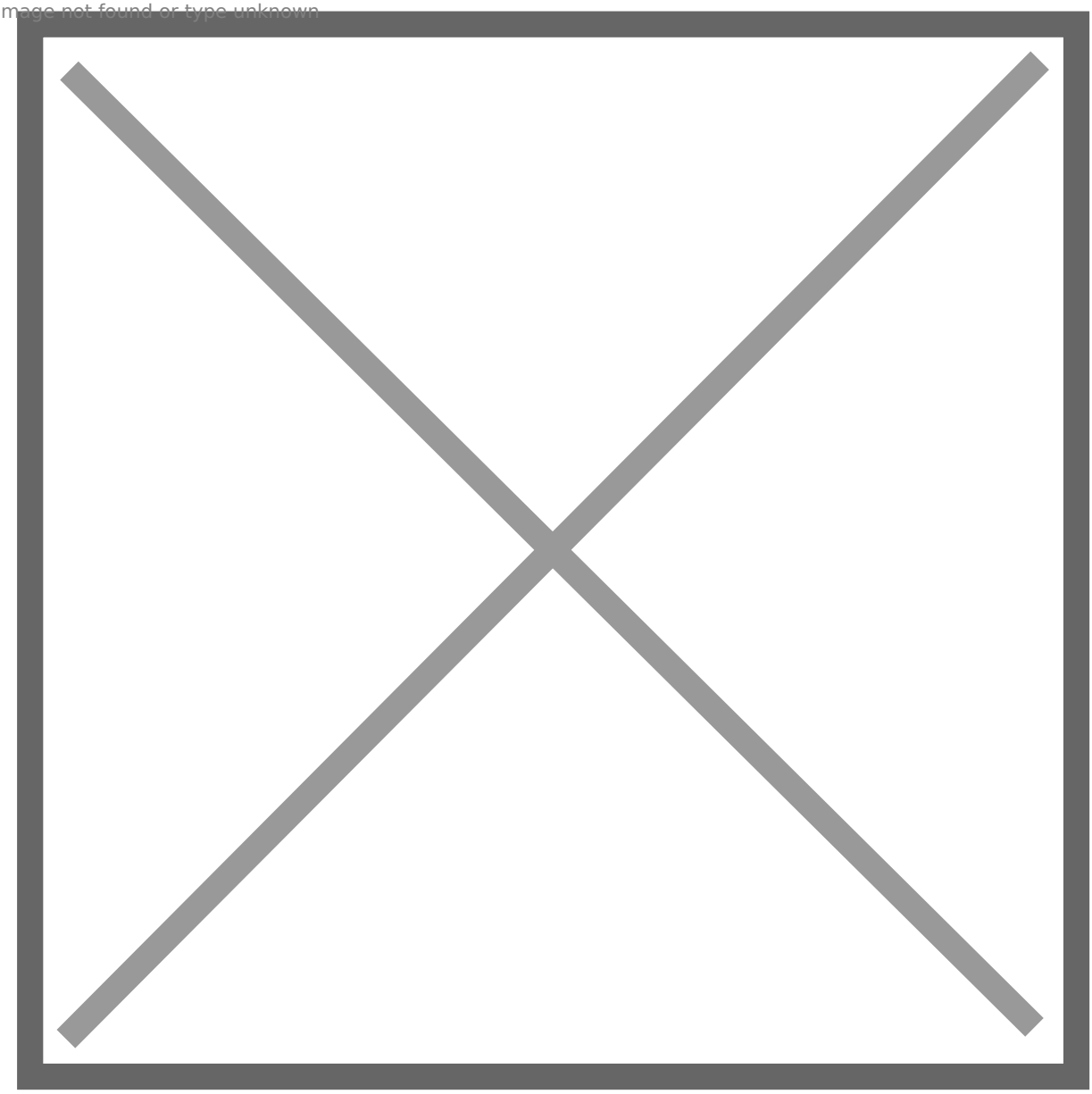
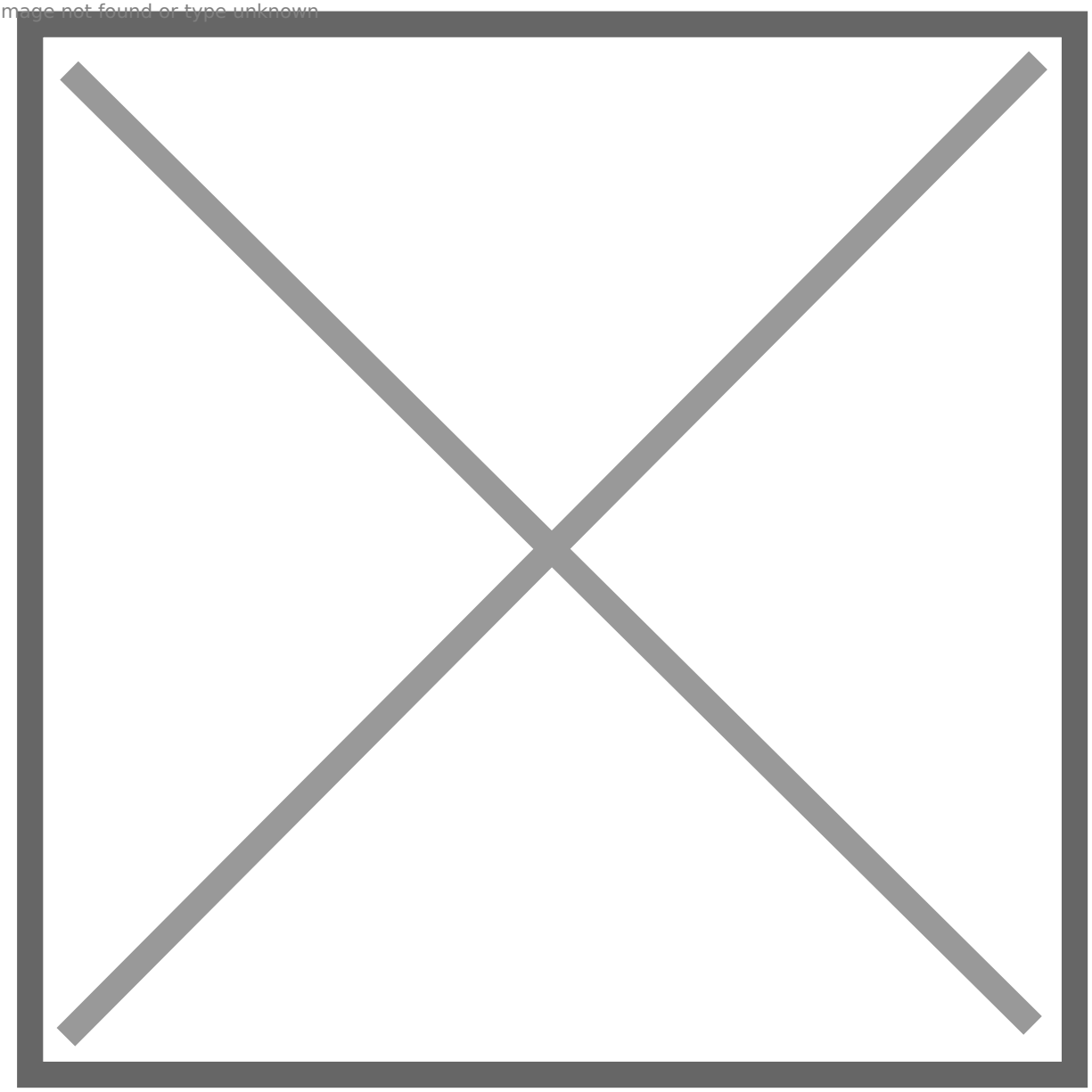


Image not found or type unknown



By following these detailed steps, you can effectively set up a site-to-site VPN connection in Azure and guide your client through the configuration process.

Congratulations! You have successfully set up a virtual network in Azure with a gateway subnet and configured a site-to-site VPN connection. By following these steps, you have established a secure connection between your Azure environment and your client’s on-premises network, allowing seamless communication between resources.

Remember to ensure that all configurations are correctly applied, and both parties have access to the necessary information, including the pre-shared key and configuration files. Regularly monitor the VPN connection status in the Azure portal to ensure smooth operation and troubleshoot any issues promptly.

With this site-to-site VPN connection in place, your organization can leverage Azure’s resources securely and extend your on-premises network to the cloud, enabling enhanced scalability, flexibility, and reliability for your infrastructure needs.

3

Microsoft License Plan Reference

https://learn.microsoft.com/en-us/entra/identity/users/licensing-service-plan-reference