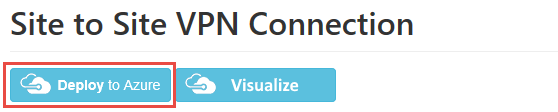
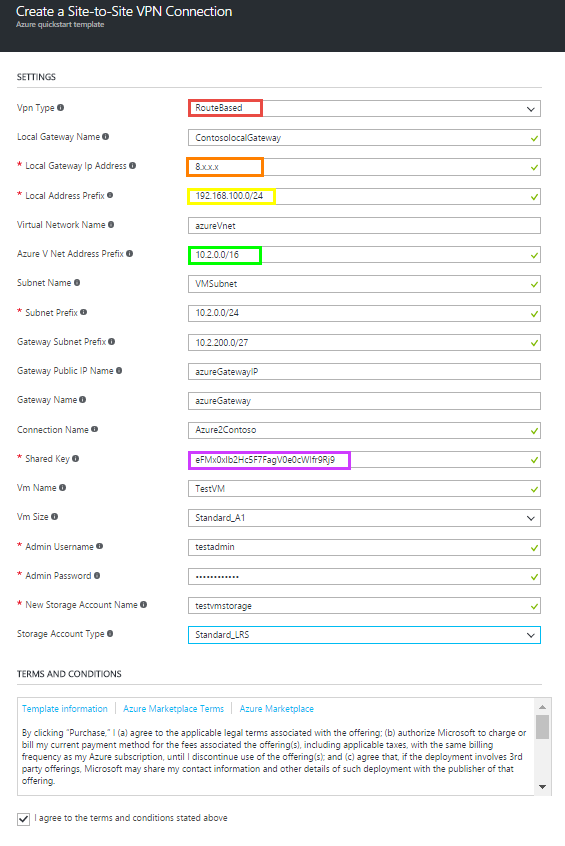
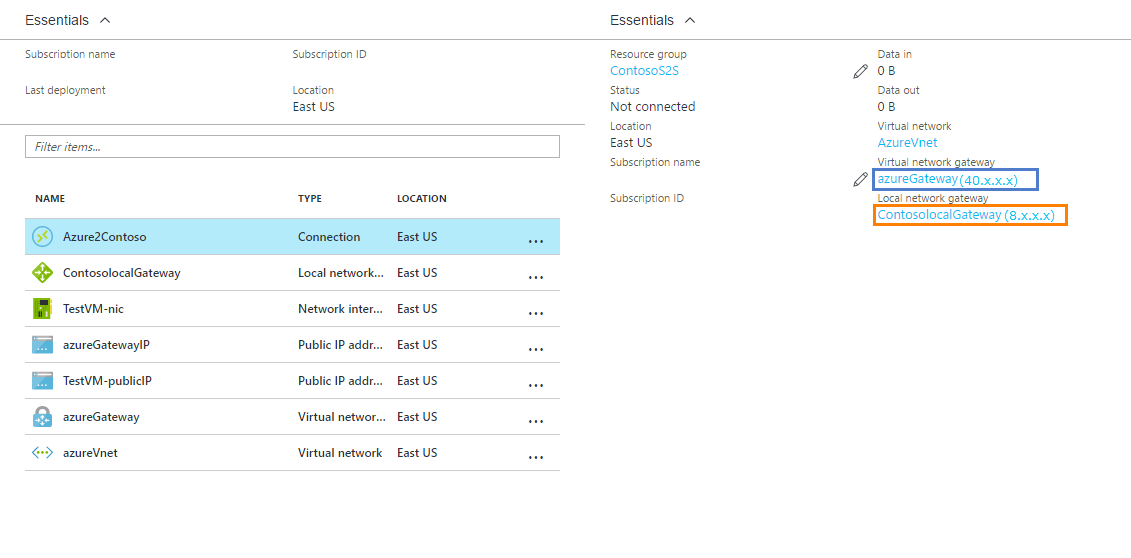
Configure azure via JSON template:



<https://github.com/Azure/azure-quickstart-templates/tree/master/201-site-to-site-vpn>



After Site 2 Site connection is deployed review your Azure gateway address and your Local gateway IP address:

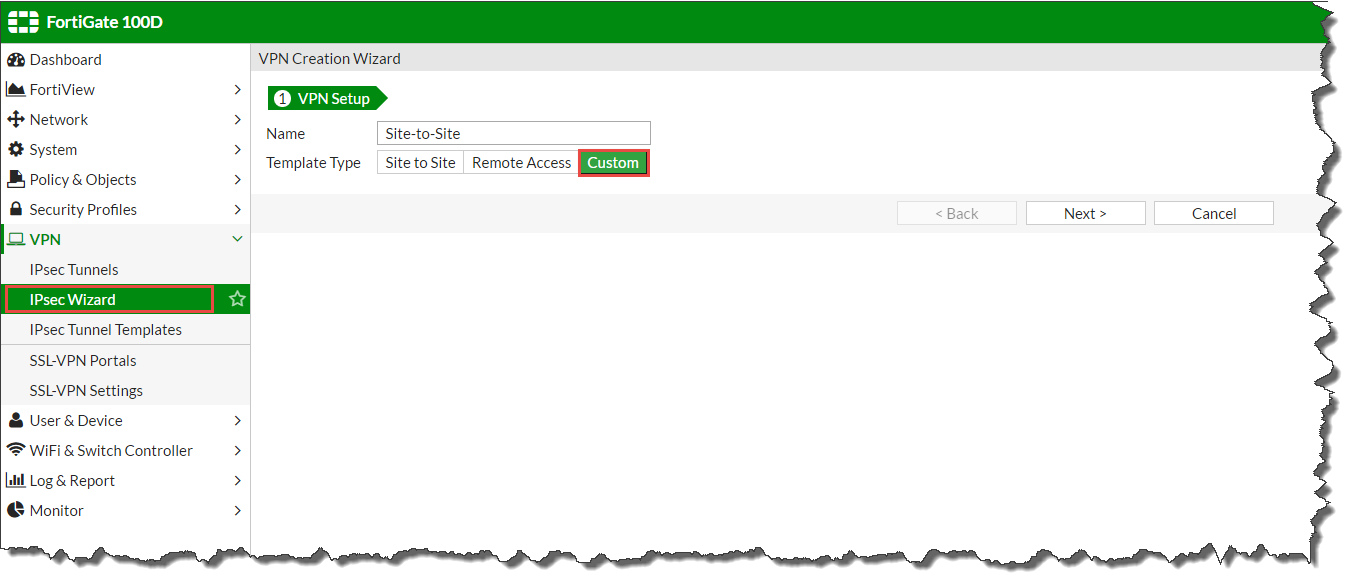


**Configure the Fortigate**

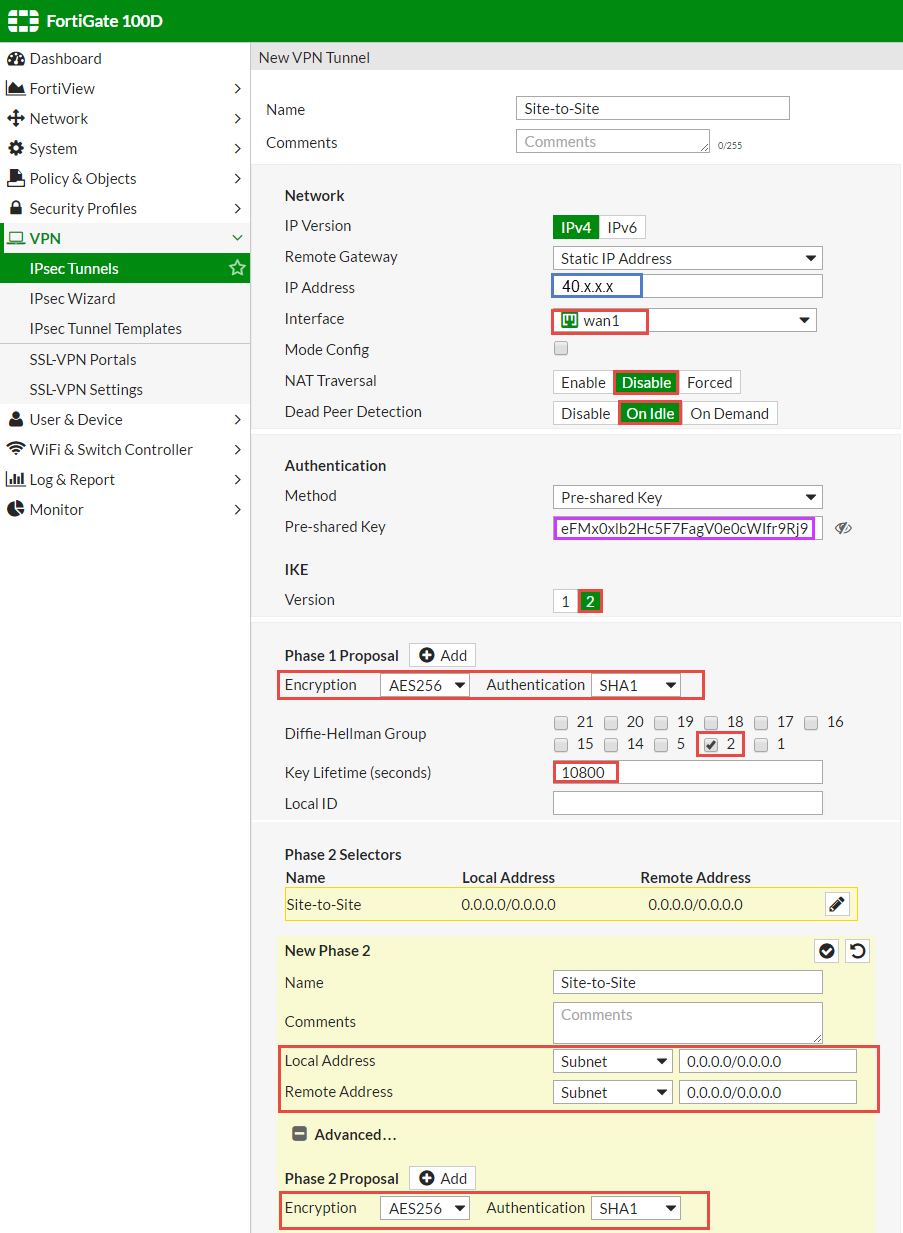
Login into the forgate mangament

Under **VPN => IPsecWizard**

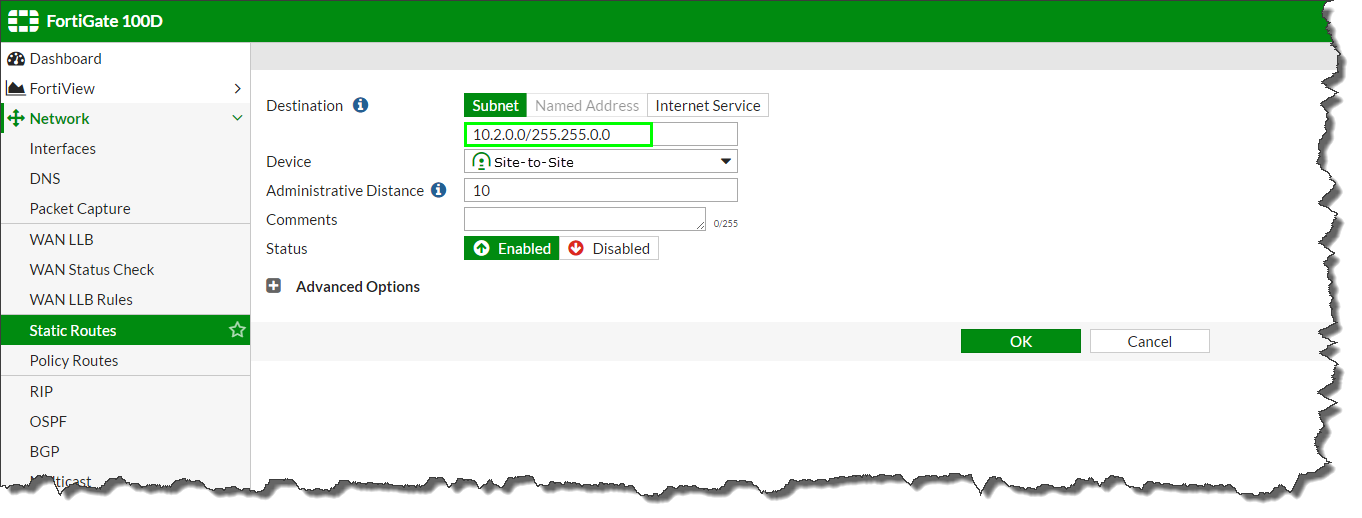
Select Custom:



Configure the VPN tunnel as outlined below:

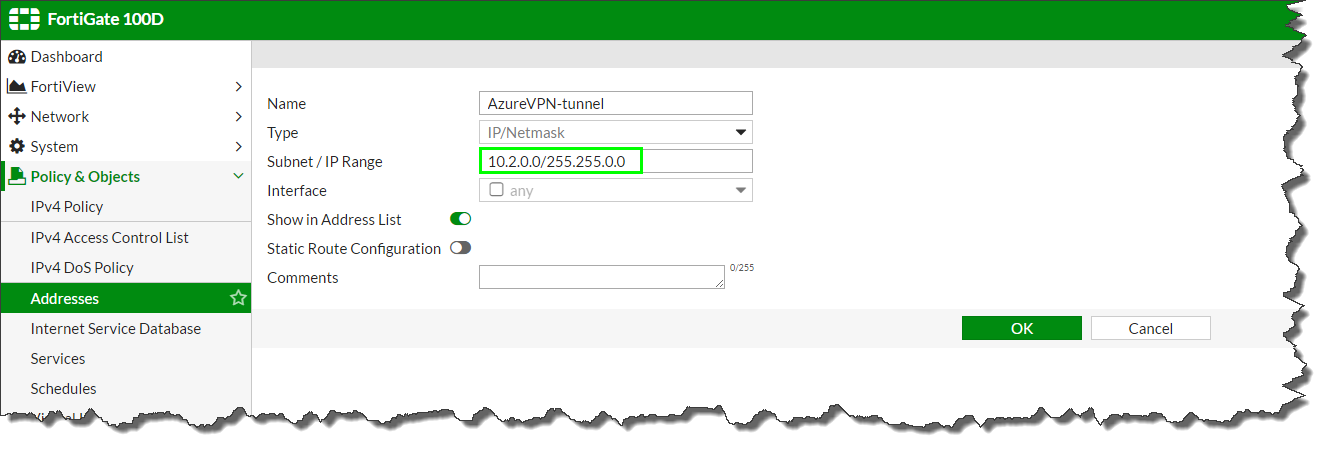


Under **Network => Static Routes**   
Create a new static route to the Azure vnet address space:

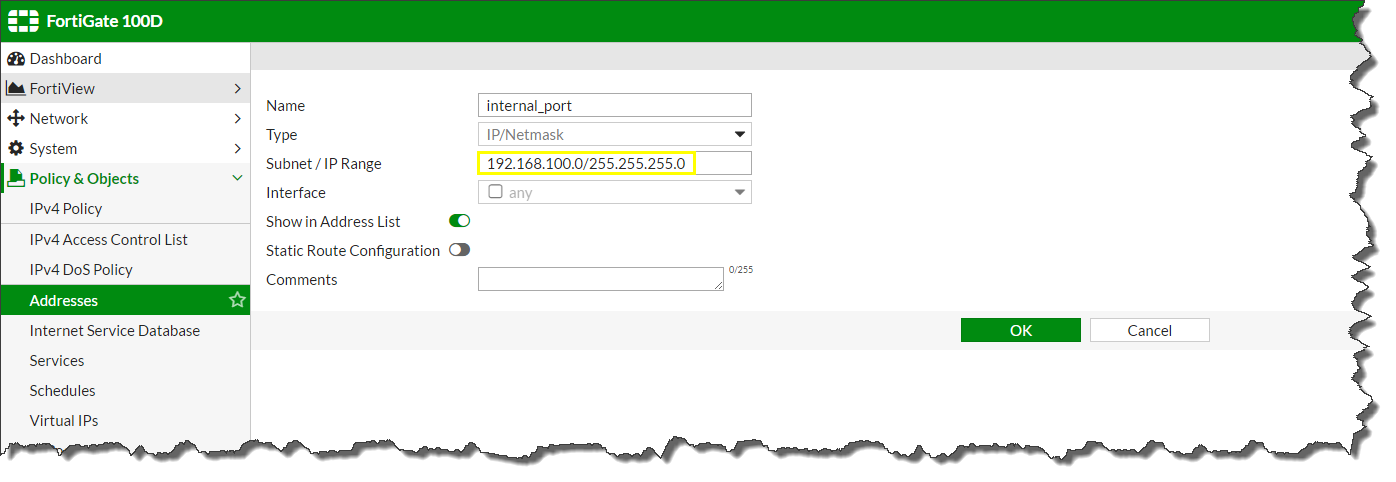


Under **Policy & Objects => Addresses**

Add the Azure vnet address space:

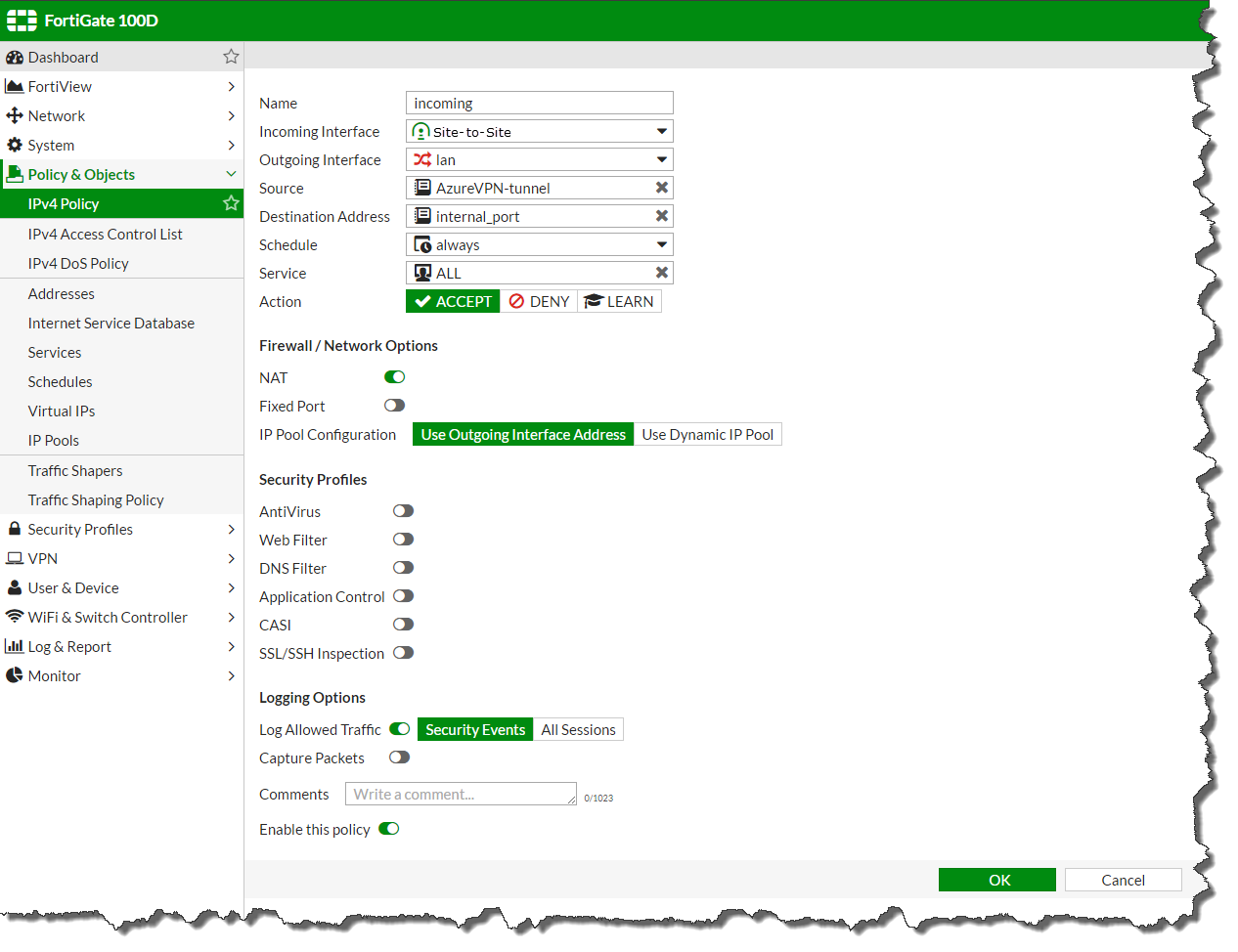


Add the Local Address space for the FortiGate:

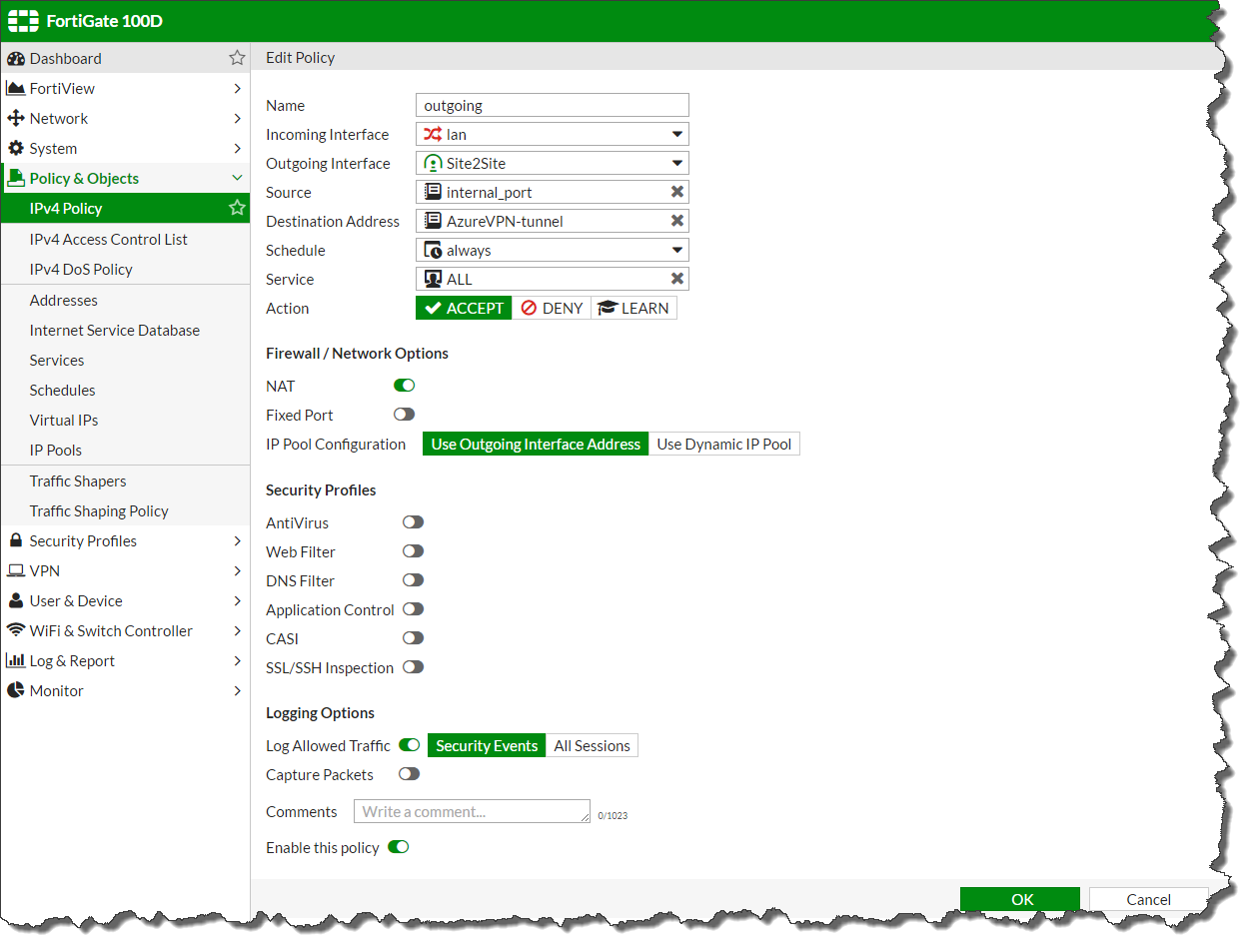


Under **Policy & Objects => IPV4 Policy**

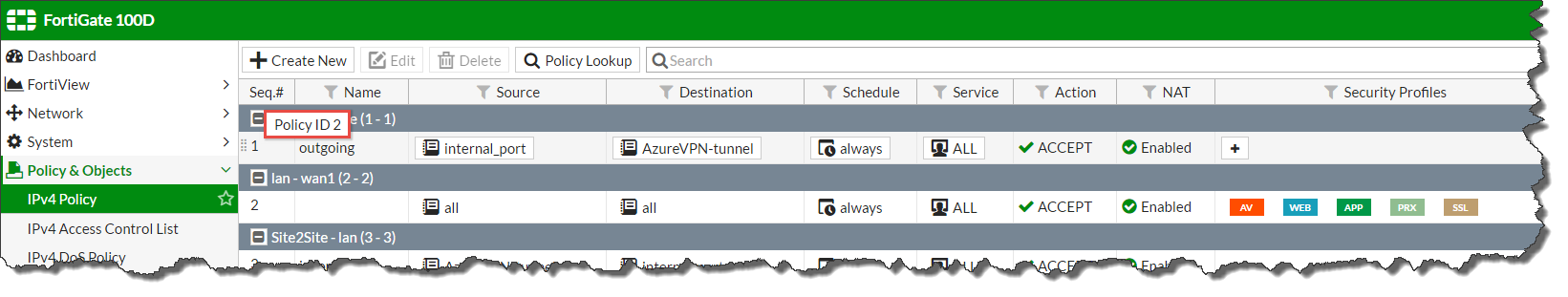
Allow the firewall to accept incoming traffic from the Azure vnet:



Create a 2nd firewall policy to allow outgoing traffic from the FortiGate to the Azure vnet:



View the policy number for outgoing by hovering your mouse over the Sequence number. In this case the Policy ID is 2:



In **Dashboard = > CLI Console**

Enter the following commands:

**config firewall policy**

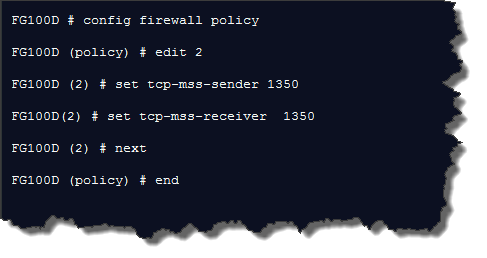
**edit 2** *(where 2 is the policy id listed above)*

**set tcp-mss-sender 1350**

**set tcp-mss-receiver 1350**

**next**

**end**

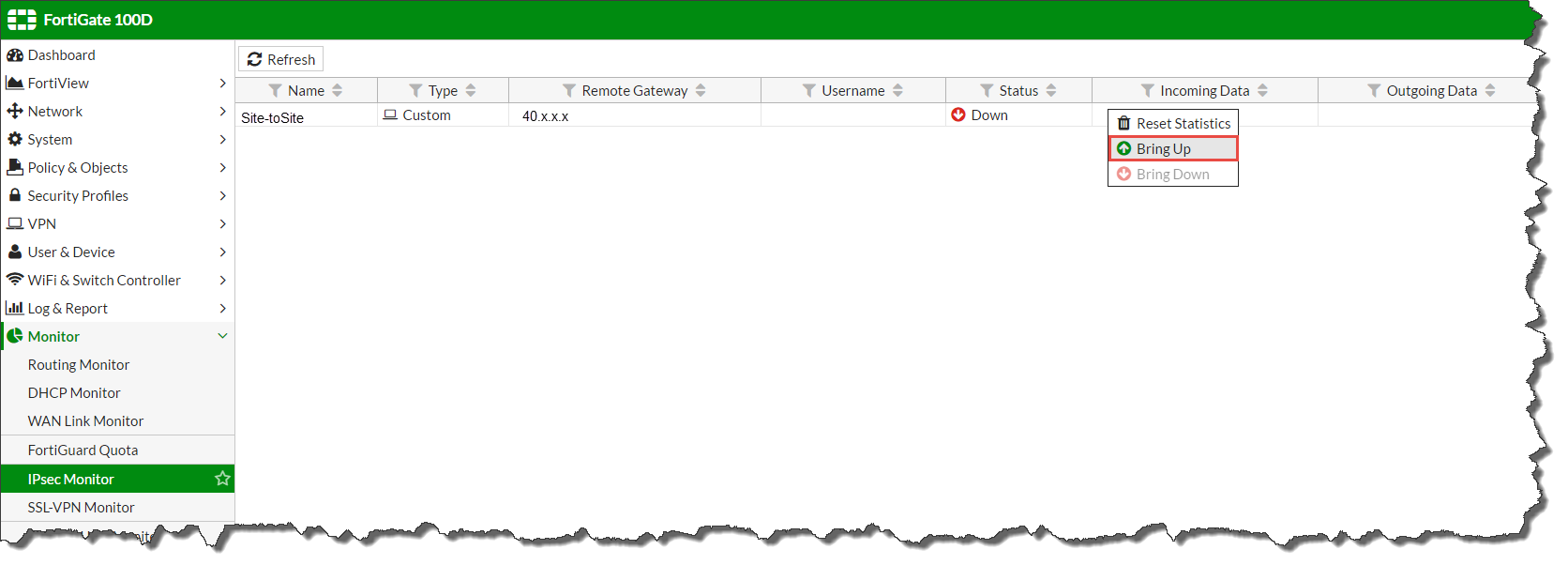


Insure your setting are correct by running **show firewall policy 2** *(where 2 is the policy id listed above)*

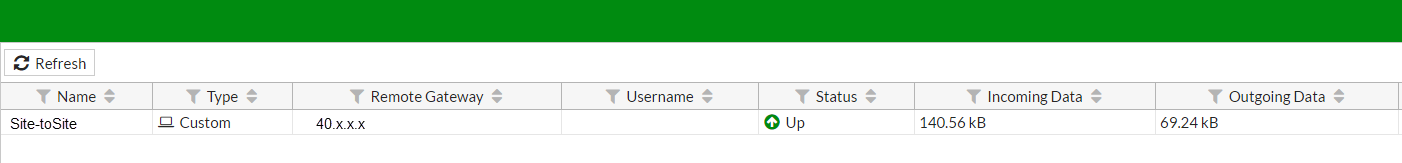


Under **Monitor => IPSec Monitor**

Right click to bring up the gateway



Ensure the VPN tunnel comes up on the FortiGate:



The Azure portal will update within a few moments

