tailscale

Read Online ↗

Access Azure Linux VMs privately using Tailscale

Microsoft Azure is a cloud service provider offering Linux and Windows virtual machines, to which Tailscale can be used to provide secure connectivity. This Knowledge Base article covers Linux VMs running within Azure.

Prerequisites

Before you begin this guide, you'll need a Tailscale network set up and configured with at least one existing device. Read our getting started guide if you need help with this.

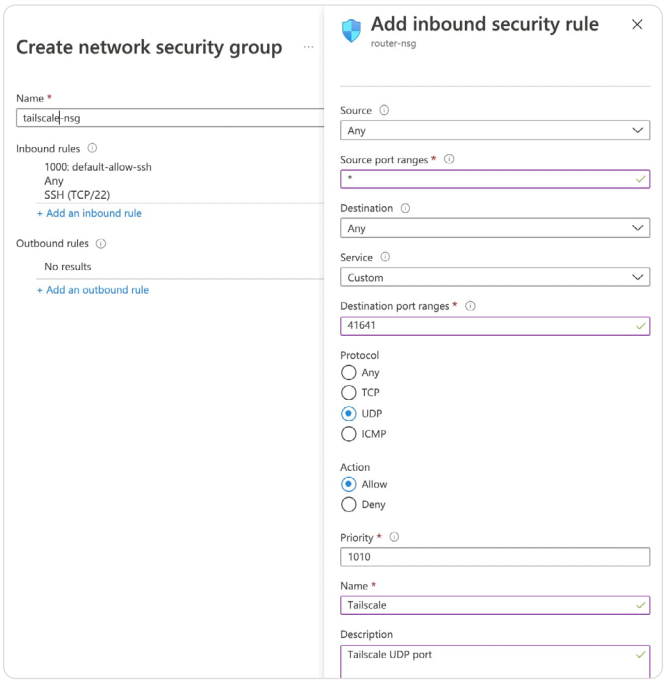
1 Set up the Tailscale client for Linux VMs

First, create a Virtual Machine in the Azure Portal running Linux. Tailscale supports many of the Linux distributions offered by Azure Marketplace images.

If at least one side of a tunnel has "easy NAT," where Tailscale can determine the UDP port number on the far side of the NAT device, then it will make direct connections to minimize latency. We ensure that the Azure nodes can make direct connections by allowing UDP port 41641 to ingress through the firewall.

In the Networking step of setting up the VM, choose Advanced for the NIC network security group and create a network security policy to allow UDP port 41641 to ingress.

Then ssh to the system and follow the steps to install Tailscale on Linux.



Networking step of setting up the VM

2 Advertise routes from the VM

For the benefit of the other nodes in the tailnet we'll set up split DNS to allow use of the same DNS names as are used inside of Azure. The Azure DNS server address is 168.63.129.16, which is an Anycasted address that will go to the nearest DNS server within Azure.

We'll have our VM advertise routes for both the subnet it sits on as well as the Azure DNS server. For example if the subnet address range is 10.1.0.0/24, the command would be:

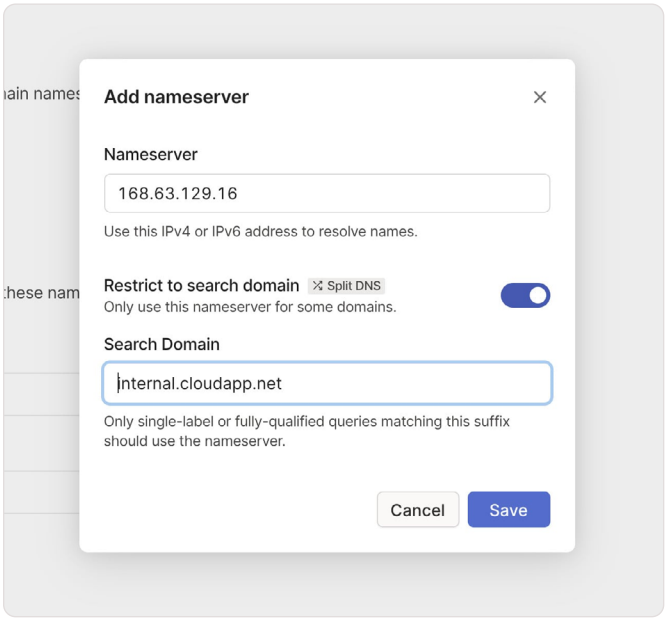
```
tailscale up --advertise-routes=10.1.0.0/24,168.63.129.16/32 --accept-dns=false
```

For Azure VMs it is generally best to let Azure handle the DNS configuration, not have Tailscale override it, so we added `--accept-dns=false`.

3 Add Azure DNS for your tailnet

In the admin console DNS section we add a nameserver restricted to the `internal.cloudapp.net` domain, pointing to the Azure DNS server which we made available through our VM.

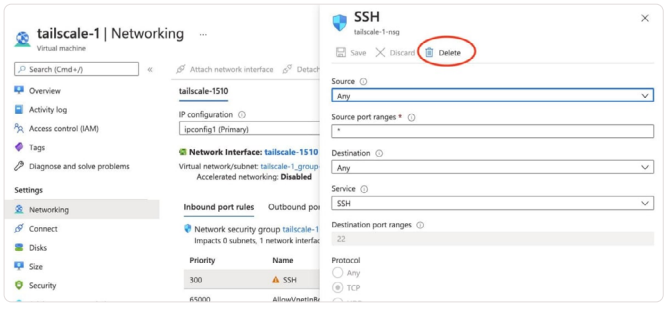
Now the same hostnames which work between nodes running within Azure will also be available to all nodes on our tailnet.



Add azure DNS for your tailnet

4 Remove public SSH access

As we can now ssh to the system over the private Tailscale network, there is no reason to leave the SSH port open on a public IP address. In the Settings > Network tab click on the ingress rule for "SSH" and delete it.



Delete the SSH ingress rule