tailscale

Read Online ↗

Access Azure Windows VMs privately using Tailscale

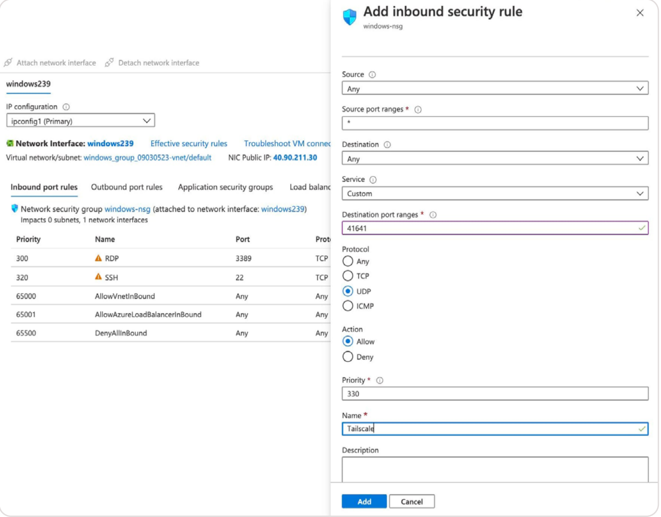
Microsoft Azure is a cloud service provider offering Linux and Windows virtual machines, to which Tailscale can be used to provide secure connectivity. This Knowledge Base article covers Windows VMs running within Azure.

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 Windows VMs

First, create a Virtual Machine running Windows Datacenter Edition.



Attach network interface · Detach network interface

windows239

IP configuration: ipconfig1 (Primary)

Network Interface: windows239 · Effective security rules · Troubleshoot VM connec

Virtual network/subnet: windows_group_09030523-vnet/default · NIC Public IP: 40.90.211.30

Inbound port rules · Outbound port rules · Application security groups · Load balanc

Network security group windows-nsg (attached to network interface: windows239)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Prot
300	⚠ RDP	3389	TCP
320	⚠ SSH	22	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule
windows-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 41641

Protocol: ○ Any ○ TCP ● UDP ○ ICMP

Action: ● Allow ○ Deny

Priority *: 330

Name *: Tailscale

Description:

Networking step of setting up the VM

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 while creating the VM choose Advanced for the NIC network security group, and create a network security policy to allow UDP port 41641 to ingress.

Then RDP to the system, and download the latest Windows installer.

It is possible to log in using a browser as described in install Tailscale on Windows, as Windows Datacenter Edition does include a GUI and web browser. However this tends not to work as well for a Cloud VM where one is likely not already logged in from the browser.

Alternately, one can use a `cmd.exe` shell to run the Tailscale CLI command and use an auth key: `tailscale up --accept-dns=false --authkey=tskey-0123456789abcdef`

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.

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.

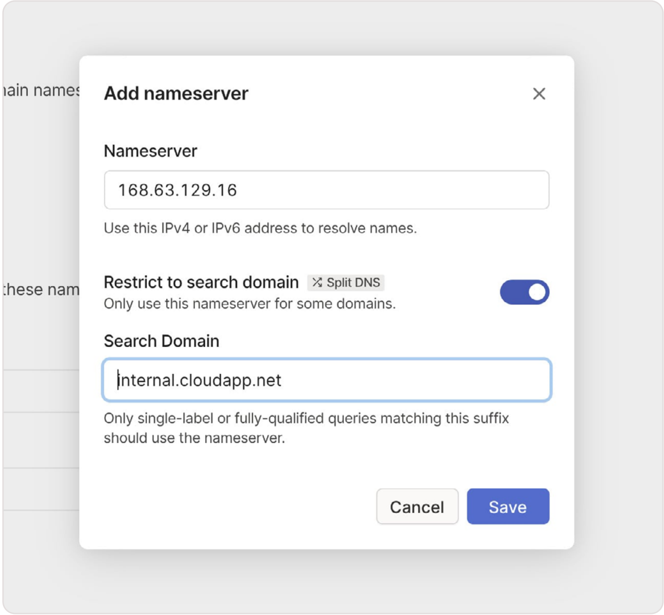
We'll use `cmd.exe` to have our VM advertise routes for both the subnet it sits on as well as the Azure DNS server. For example if the subnet address range is 10.1.0.0/24, the command would be:

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

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 nameserver

Nameserver: 168.63.129.16

Use this IPv4 or IPv6 address to resolve names.

Restrict to search domain (on)
Only use this nameserver for some domains.

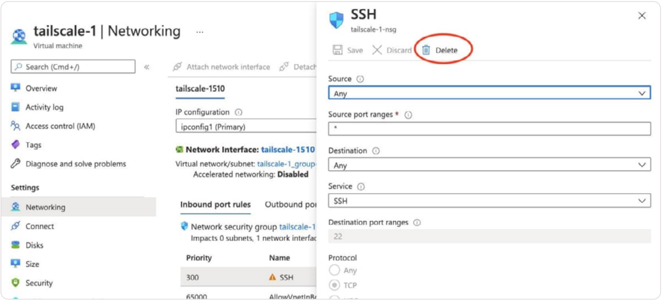
Search Domain: internal.cloudapp.net

Only single-label or fully-qualified queries matching this suffix should use the nameserver.

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.



IP configuration: ipconfig1 (Primary)

Network Interface: tailscale-1510
Virtual network/subnet: tailscale-1_group-
Accelerated networking: **Disabled**

Network security group tailscale-1
Impacts 0 subnets, 1 network interfac

Priority	Name
300	SSH
65000	AllowVnetInB

Source: Any

Source port ranges *: *

Destination: Any

Service: SSH

Destination port ranges: 22

Protocol
○ Any
● TCP

Delete the SSH ingress rule