:: tailscale

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 <u>getting started guide</u> if you need help with this.

1 Set up the Tailscale client for Linux VMs

First, <u>create a Virtual Machine in the Azure Portal</u> running Linux. Tailscale supports <u>many of the Linux distributions</u> 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 <u>direct connections to</u> <u>minimize latency</u>. 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.

2 Advertise routes from the VM

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

Create network security group	Add inbound security rule	×
Name *		
tailscale-nsg	Source ①	
Inbound rules O 1000: default-allow-ssh Any SSH (TCP/22)	Any Source port ranges * ① *	~
+ Add an inbound rule	Destination ()	
Outbound rules ①	Any Service ①	\sim
No results	Custom	~
+ Add an outbound rule	Destination port ranges * ①	
	41641	~
	Protocol Any TCP UDP ICMP	
	Action Allow	
	Deny Priority *	
	1010	
	Name *	
	Tailscale	~
	Description	
	Tailscale UDP port	~

Networking step of setting up the VM

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 <u>admin console DNS section</u> 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.

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.

iain names	Add nameserver ×
	Nameserver
	168.63.129.16
	Use this IPv4 or IPv6 address to resolve names.
hese nam:	Restrict to search domain × Split DNS Only use this nameserver for some domains.
	Search Domain
	İnternal.cloudapp.net
	Only single-label or fully-qualified queries matching this suffix should use the nameserver.
	Cancel Save

Add azure DNS for your tailnet

tailscale-1 Networ	king …	SSH talscale-1-nsg	×
P Search (Cmd+/) ≪	${\mathscr G}$ Attach network interface ${\mathscr G}^{{\mathbb C}}$ Detach		
Overview	tailscale-1510	Source 🕜	~
Activity log	IP configuration ()	Source port ranges * (i)	
Access control (IAM)	ipconfig1 (Primary)	•	
🔷 Tags	S Network Interface: tailscale-1510	Destination ③	
Diagnose and solve problems	Virtual network/subnet: tailscale-1_group Accelerated networking: Disabled	Any	~
Settings		Service ①	
Setworking	Inbound port rules Outbound por	SSH	~
Ø Connect	Retwork security group tailscale-1	Destination port ranges ③	
Disks	Impacts 0 subnets, 1 network interfac	22	
Size	Priority Name	Protocol	
© Security	300 🔺 SSH	Any TCP	
	65000 Allow/VnetinBr		

Delete the SSH ingress rule