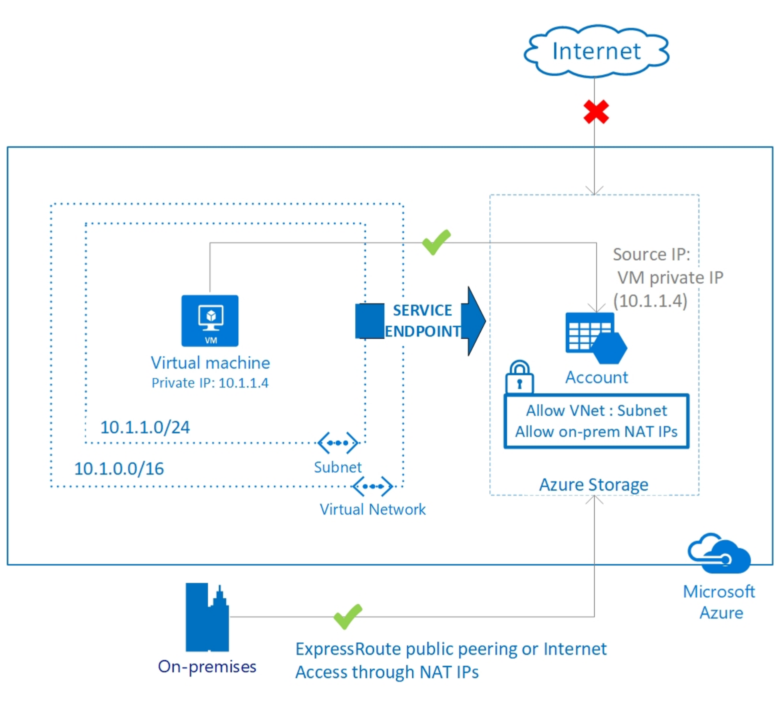
INTERNET ARCHIVE WayBackMachine
https://www.fugue.co/blog/cloud-network-security-101-azure-virtual-network-service-endpoints
11 captures
6 Oct 2020 – 9 Jun 2023
DEC JAN APR
2020 27 2021 2022
About this capture

Cloud Network Security 101: Azure Virtual Network Service Endpoints

Becki Lee | September 17, 2020



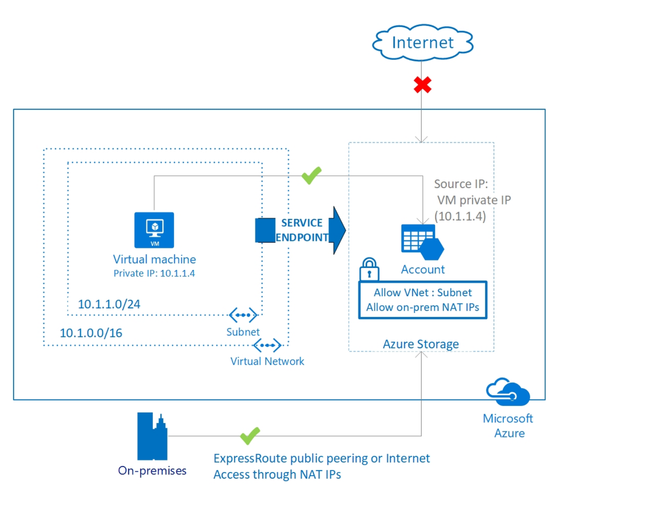
Microsoft Azure offers two similar but distinct services to allow virtual network (VNet) resources to privately connect to other Azure services. Azure VNet Service Endpoints and Azure Private Endpoints (powered by Azure Private Link) both promote network security by allowing VNet traffic to communicate with service resources without going over the internet, but there are some differences.

This three-part blog series goes into detail about both services.

- In part 1 of this series **(this part!)**, we'll talk about service endpoints.
- In part 2, we'll go over Private Link and private endpoints.
- In part 3, we'll compare and contrast the two and explain when to use which.

Ready to learn about Azure service endpoints? Let's dive in!

What is an Azure service endpoint?



Above, the virtual machine has the private IP address 10.1.1.4 but can access the storage account over a service endpoint.

On-premises traffic cannot use service endpoints, and must go over the internet to access the storage account. Image from https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#secure-azure-services-to-virtual-networks

A service endpoint allows VNet resources to use *private* IP addresses to connect to an Azure service's *public* endpoint, meaning traffic flows to the service resource **over the Azure backbone network -- instead of over the internet**. In effect, you are extending the identity of the VNet to the service resource. You can then lock down the service resource so it only accepts traffic from the subnet associated with the service endpoint.

Optionally, you can lock down the VNet as well by adding a network security group (NSG) to deny all outbound traffic except to the desired Azure service. With the right configuration, service endpoints enable you to secure service resources to your VNet, providing an extra layer of security.

For example, say you have a virtual machine (VM) in a VNet that needs to communicate with an Azure storage account. You can combine a service endpoint, storage account, and NSG so that traffic from a VM in a private subnet reaches the storage account without hitting the internet, the storage account blocks all traffic unless it's from that subnet, and the NSG restricts outbound traffic from the subnet to the internet.

Without a service endpoint, the VM would need to be assigned a public IP address, exposing it to the internet and all the threats that go along with it; the subnet would need a NAT gateway device, requiring an extra step of configuration and potentially slowing traffic; and the storage account would need to be open to clients on any network, so if credentials are leaked, anyone on the internet can access it. Hardly ideal!

Fugue
The Engineer's Handbook on Cloud Security
A primer on securing your cloud infrastructure and demonstrating compliance
GET THE HANDBOOK

Now, let's look at some of the benefits that service endpoints introduce:

- **Enhanced security:** Because the virtual network resource uses a private IP address to connect to the service resource, there's no need to assign it a public IP address. Without a public IP address, malicious actors can't scan a VM's open ports for vulnerabilities and bring down your application or steal data.
- **Optimized routing:** The service endpoint provides a direct route over the Azure backbone network from the VNet to the service resource, so there are no extra hops to slow down traffic.
- **Simpler network architecture:** Since traffic flows from the VNet resource to the service resource over the Azure backbone network, you don't need to give it a public IP address or configure a NAT or gateway device. Plus, you can enable a service endpoint in a couple of clicks, and Azure handles the behind-the-scenes work of maintaining it.

Service endpoints are currently available for PaaS services such as Azure Storage, Azure SQL Database, Azure Key Vault, and others.

Azure service endpoint policies

By default, every storage account has a network access rule that allows traffic from all networks, including the internet. To protect your storage account `mystorageaccount`, you can enable a service endpoint and then modify `mystorageaccount`'s default network access rule to deny traffic unless it's from the service endpoint. (We'll explain how to do this shortly.) In this case, `vm1` in the service endpoint's subnet can access `mystorageaccount`, but `vm2` in a different subnet can't access `mystorageaccount`. This is because service endpoints are enabled per service, per subnet.

Modifying `mystorageaccount`'s ACL in such a way protects `mystorageaccount` from internet traffic, but it's important to note that a service endpoint allows any compute instance in the associated subnet to access other available storage accounts (again, because service endpoints are enabled per service, per subnet). If a bad actor in your organization secretly configures `roguestorageaccount` to allow traffic from the service endpoint, `vm1` can send traffic to it, allowing the bad actor to exfiltrate data -- even if `roguestorageaccount` is in a different subscription or Active Directory tenant.

Fortunately, Azure provides a solution for that exact scenario: service endpoint policies (currently only enabled for Azure Storage resources). A service endpoint policy specifies the scope of the service endpoint: it only allows access to all storage accounts in a subscription, all storage accounts in a resource group, or a single storage account.

By using a service endpoint policy to designate more precisely where traffic can go, you can reduce the risk of data exfiltration. In this example, you can configure the service endpoint to allow `vm1` to send traffic only to `mystorageaccount`, and not `roguestorageaccount`.

Similarity to AWS VPC endpoints

If you're an AWS user and all of this sounds familiar to you, you might be thinking of VPC gateway endpoints, which also use routes to secure storage and database resources to a subnet in a virtual network without requiring traffic to go over the internet. Gateway endpoints also grant full access from the subnet to the service unless you apply an endpoint policy to narrow down which resources can be accessed -- much like the way you'd use Azure service endpoint policies.

How to create an Azure service endpoint

You can set up a service endpoint in two easy steps:

1. Enable the service endpoint on the network side
2. Configure ACLs on the service resource side

Here's a quick walkthrough, which is an abbreviated version of this excellent Azure tutorial. Let's say you have a VM in a private subnet in a virtual network, and a storage account in the same region, and you want traffic to flow from the former to the latter without going over the internet.

Enable the service endpoint on the network side:

1. Navigate to the subnet and edit it.
2. Select "Microsoft.Service" under the "Service endpoints" heading.
3. Select "Save."

Modify the default network access rule on the storage account side:

1. Navigate to the storage account and select "Firewalls and virtual networks" in the sidebar. Under "Allow access from," select "Selected networks."
2. Select "Add existing virtual network," then choose the virtual network and subnet you just edited.
3. Select "Add" and then "Save."

That's it! You just enabled a service endpoint. If you'd like to test it out, create a network security group (NSG) with an inbound rule allowing SSH or RDP access from only your home IP address, and associate it with the service endpoint subnet. (You can use whatismyip.com to find your IP address. Note that the VM will need a public IP address as well in order for you to reach it from home.) SSH or RDP into the instance and try to access the storage account, such as by listing its containers using the Azure CLI or PowerShell. You'll see that you can reach the storage account from the VM, and you can't from your own IP address. (If you create another VM in the same subnet, it'll also have access to the storage account, because a service endpoint without a service endpoint policy allows any resource in the associated subnet to access other available storage accounts.)

For bonus points: Implement a tactic we mentioned earlier by locking the NSG down so outbound traffic from the VM is blocked to the internet. You can do this by creating two outbound security rules: one to allow outbound traffic only to Azure Storage, and another to block outbound traffic to the internet.

First, create an outbound security rule with the following configuration to allow traffic to Azure Storage:

- Source: **VirtualNetwork**
- Destination: **Service Tag**
- Destination service tag: **Storage**
- Destination port ranges: * (asterisk)
- Action: **Allow**
- Priority: **100**

Enter a new name, and keep the other defaults. Then create another outbound security rule with the following configuration to block traffic to the internet:

- Source: **VirtualNetwork**
- Destination: **Service Tag**
- Destination service tag: **Internet**
- Destination port ranges: * (asterisk)
- Action: **Deny**
- Priority: **110**

Enter a new name, and keep the other defaults. Voila! The VM can only accept traffic from your IP, it can only send traffic to Azure Storage, and the target storage account only accepts traffic from the service endpoint.

For the full walkthrough, see Azure's article Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
.

Extra credit: Set up a service endpoint policy so the VM can send traffic to *only* the desired storage account, instead of *any* available storage account. Here's another great Azure tutorial that shows you how.

Things to know before you use service endpoints

A few tips to keep in mind about service endpoints:

- There's no cost for service endpoints. You're charged for the VNet resources and service resources you use, as always, but you pay nothing extra for service endpoints.
- As discussed earlier, a service endpoint is implemented for an entire service (and, depending on the service, it doesn't even need to be the same AD tenant). However, if your service resource is a storage account, you can use a service endpoint policy to narrow the scope to all storage accounts in a subscription or resource group, or to a single storage account.
- When you enable a service endpoint, VMs in the associated subnet switch from public IP addresses to private IP addresses. Keep this in mind, as existing firewall rules set to public IP addresses can fail. Additionally, traffic from the subnet to the service resource might be temporarily interrupted during the switch, so make sure critical tasks aren't running when you enable or disable a service endpoint!
- Service resources can only be secured to virtual networks, so on-premises traffic can't use service endpoints to connect to an Azure service. (If you want to allow traffic from on prem, don't despair; check back for part 2 of this tutorial, where we discuss Private Link and private endpoints!)

Conclusion

As you can see, service endpoints are an excellent way to secure your VNet and service resources by extending your VNet's identity to the service resource. The traffic source is a private IP address and the destination is the service resource's public IP address.

But what if you want the destination to be a private IP address, too?

That's where Private Link and private endpoints come in. Stay tuned for part 2 of this blog series!

Fugue
Cloud Security Masterclass
Security Education for Engineers and IT Professionals on S3, IAM & more
GET STARTED

SEARCH

Search

RELATED POSTS

Fugue Now Supports Microsoft Azure to Provide Multi-Cloud Security Posture Management
July 17, 2019

Cloud Network Security 101: AWS VPC Endpoints
September 12, 2019

Cloud Network Security 101: AWS Security Groups vs NACLs
September 19, 2019

Securing Microsoft Azure Virtual Networks and Network Security Groups
November 1, 2019

Cloud Network Security 101: Azure Private Link & Private Endpoints
September 25, 2020

Cloud Network Security 101: Azure Service Endpoints vs. Private Endpoints
October 8, 2020

POPULAR CATEGORIES

Security & Compliance | Cloud | AWS | Fugue | cloud security

Featured Posts

Introducing the Engineer's Handbook on Cloud Security
Drew Wright
August 26, 2020

3 Big Amazon S3 Vulnerabilities You May Be Missing
Drew Wright
May 21, 2020

Cloud Security for Newly Distributed Engineering Teams
Drew Wright
March 19, 2020

Fugue Developer
Free Cloud Security for Engineers
- Visualize your cloud infrastructure
- Run policy checks and get feedback
- Detect change and eliminate misconfiguration
GET STARTED CONTACT SALES

Company: About, Customers, Press, Events, Careers, Security, Privacy Policy
Product: Login, Pricing, Overview, API, Documentation, Submit a Ticket
Resources: Blog, Cloud Security, Cloud Compliance, Case Studies, Library

Subscribe to our newsletter:
Subscribe

GET DEMO CONTACT US

©2021 Fugue, Inc.