Integrating Data Services with Virtual Networks

John Savill
TECHNICAL ARCHITECT

@ntfaqguy https://savilltech.com

Module Overview

Virtual Network Injection

Using Service Endpoints for Routing

Restricting Service Access from Virtual Networks with NSGs

Restricting Service Access Using Service Endpoint Policies

Restricting Traffic Using NVAs and Azure Firewall

Virtual Network Injection

- One approach to restrict access to services is to:
  - Deploy the service into the virtual network
  - Enable the service to have an adapter in the virtual network
- With the service injected into the virtual network it is possible to remove the public access, i.e. from the Internet
- It also enables additional traffic control options such as using NSGs and NVAs
- Azure IaaS VM based services are deployed into VNets
- Azure SQL Managed Instance deploys into a VNet and by default is exposed only via the private IP

Using Service Endpoints

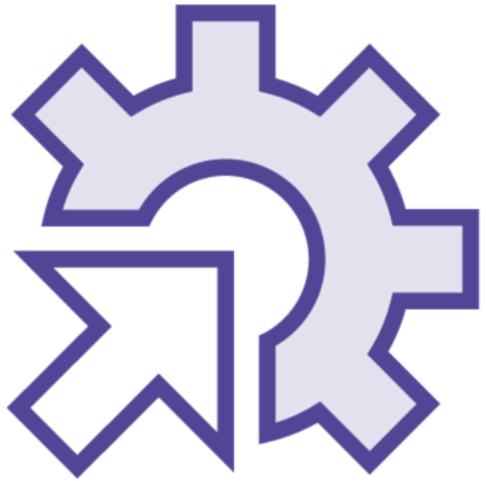
For services that cannot integrate with a virtual network many can still have optimal routing defined

- In addition to enhancing security but that is the next module!

When using service endpoints traffic is routed using the most optimal route to the service on the Azure backbone

To utilize service endpoints:

- Create service endpoint for subnets on a virtual network for supported services
- On the service instance enable access for the subnet



Controlling Access from Virtual Networks with Network Security Groups

- Network Security Groups (NSGs) enable segmentation (and micro-segmentation) for Virtual Networks
- Rules are traditionally based on IP addresses
- Service Tags can also be used in rules that denote services like the Internet, Azure Load Balancer, known network space and other Azure services, such as Azure Storage
- Service Tags for many services can also be region specific, for example Storage.EastUS
- The use of Service Tags for Azure services remove the need to try and track all possible IP addresses that service may use
- This enables control on which services can be utilized from the virtual network

Service Endpoint Policies

Allows more granular control enabling access to not only a type of service and region but also outbound to specific instances, i.e. a resource URI

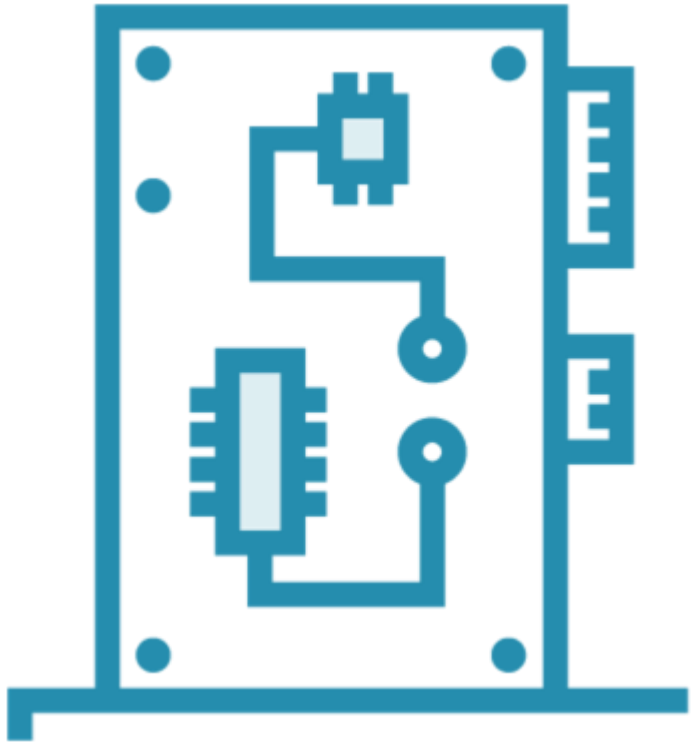
This is in a limited preview today

Service endpoint policies are a distinct resource that is created and managed

Policies are applied at a subnet level

Multiple policies can be applied to a single subnet

Azure Private Link



Azure Private Link enables private endpoints to be created in target virtual networks that represents a service instance

Private endpoint uses an IP from the target vnet

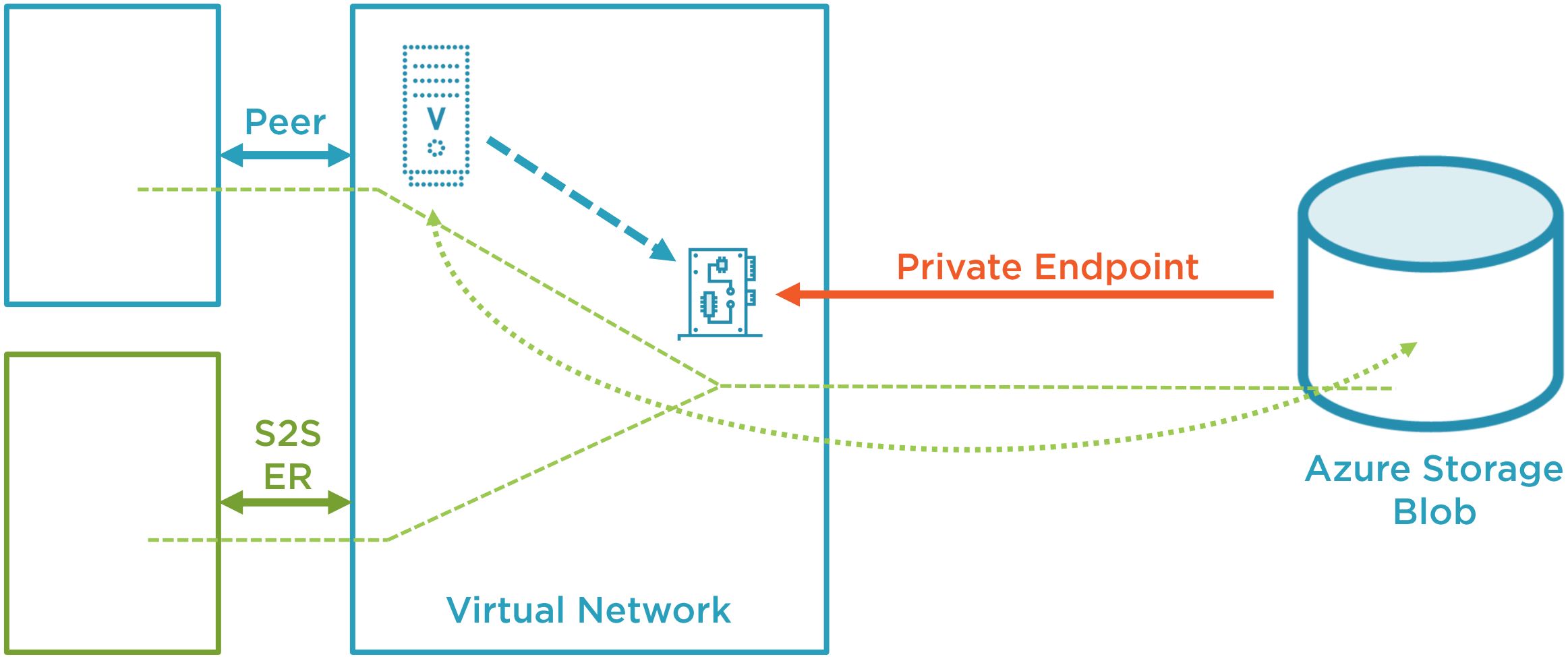
Provides the most direct path from the vnet connected resources and the target service

Can be used with

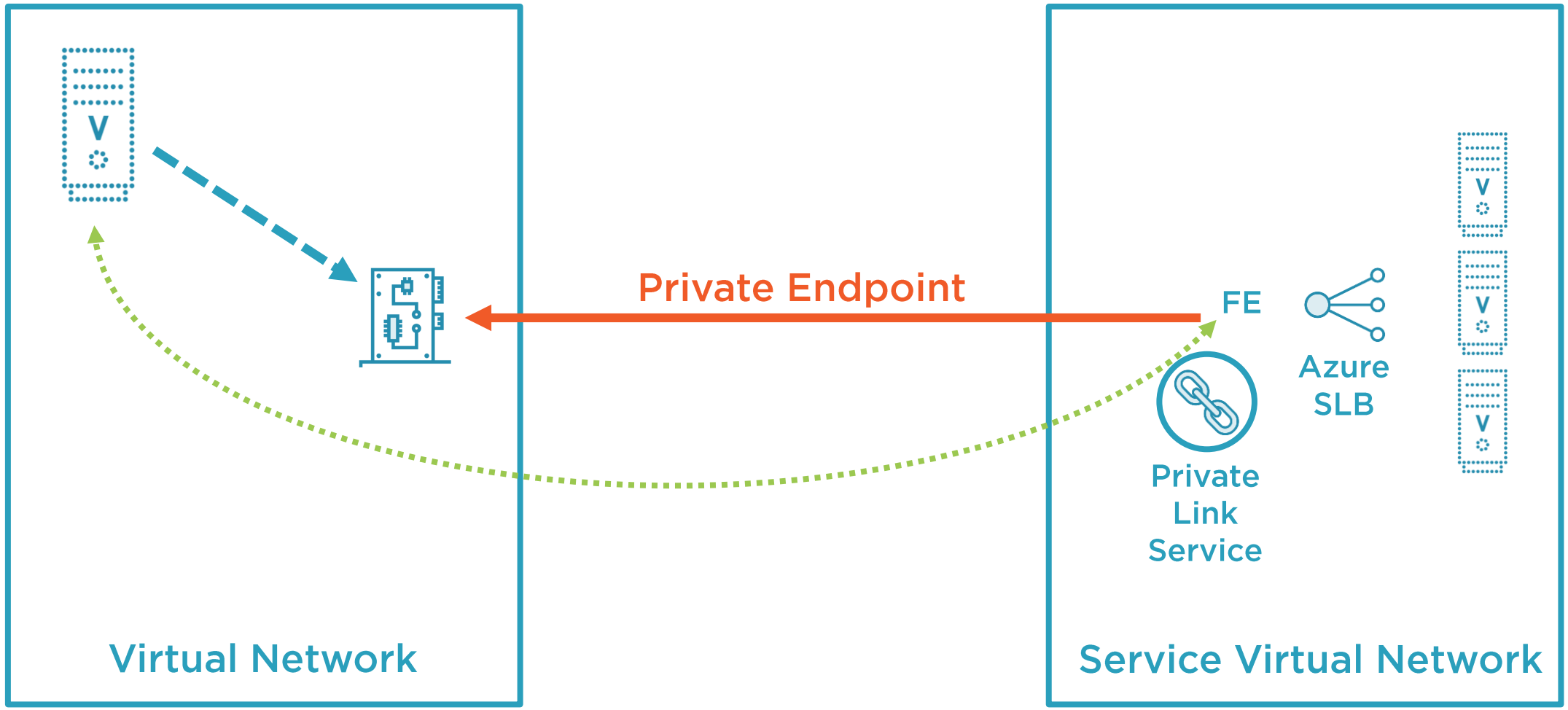
- Many Azure PaaS services, e.g. Azure Storage, avoiding the need to have public endpoints
- Custom services behind Azure Standard Load Balancer

Private Link endpoints are to a specific service instance which helps protects against data exfiltration

Azure PaaS Private Endpoint



Azure PaaS Custom Endpoint



Azure Private Link DNS Planning

Azure PaaS services have a public endpoint and public DNS name which varies by service, e.g. <SA Name>.blob.core.windows.net

The IP address of the endpoint cannot be used as the certificate would be invalid

When Private Link endpoint is enabled the DNS name now points to two aliases

- <SA Name>.privatelink.blob.core.windows.net
- <SA Name>.blob.core.windows.net

The privatelink record points to the endpoint IP

If using Azure DNS then Azure Private DNS can be used for the privatelink zone

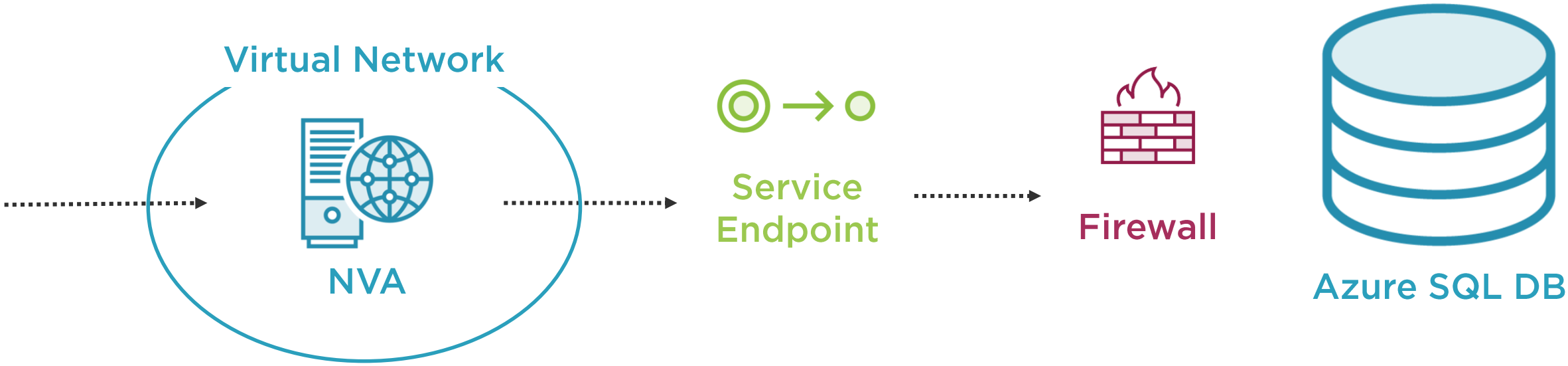
Utilizing NVA or Azure Firewall

Can deploy NVA/Azure Firewall to a virtual network

The subnet can be enabled for a service using service endpoints

All traffic must then flow via the NVA/Azure Firewall

This is commonly used when accessing services from on-premises



Module Overview

VNet Injection

Using Service Endpoints for Routing

Restricting Service Access from VNets with NSGs

Restricting Service Access Using Service Endpoint Policies

Restricting Traffic Using NVAs and Azure Firewall

Next Up:
Securing Resource Endpoints