Microsoft Azure Network Engineer: Design and Implement Routing

Design, Implement, and Manage VNet Routing

Tim Warner

Principal Author Evangelist, Pluralsight

@TechTrainerTim TechTrainerTim.com

Overview

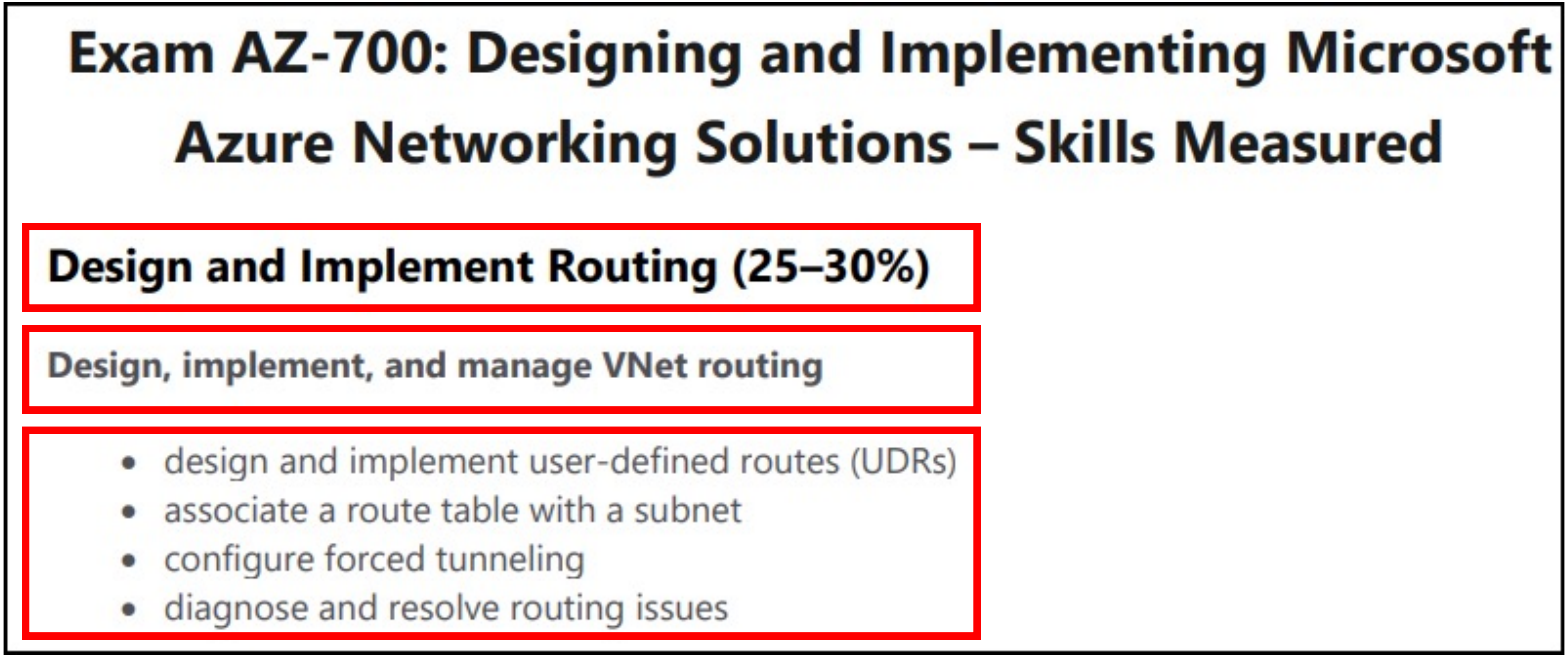
Design and implement user-defined routes (UDRs)

Associate a route table with a subnet

Configure forced tunneling

Diagnose and resolve routing issues

Relevant Exam AZ-700 Skills



Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions – Skills Measured

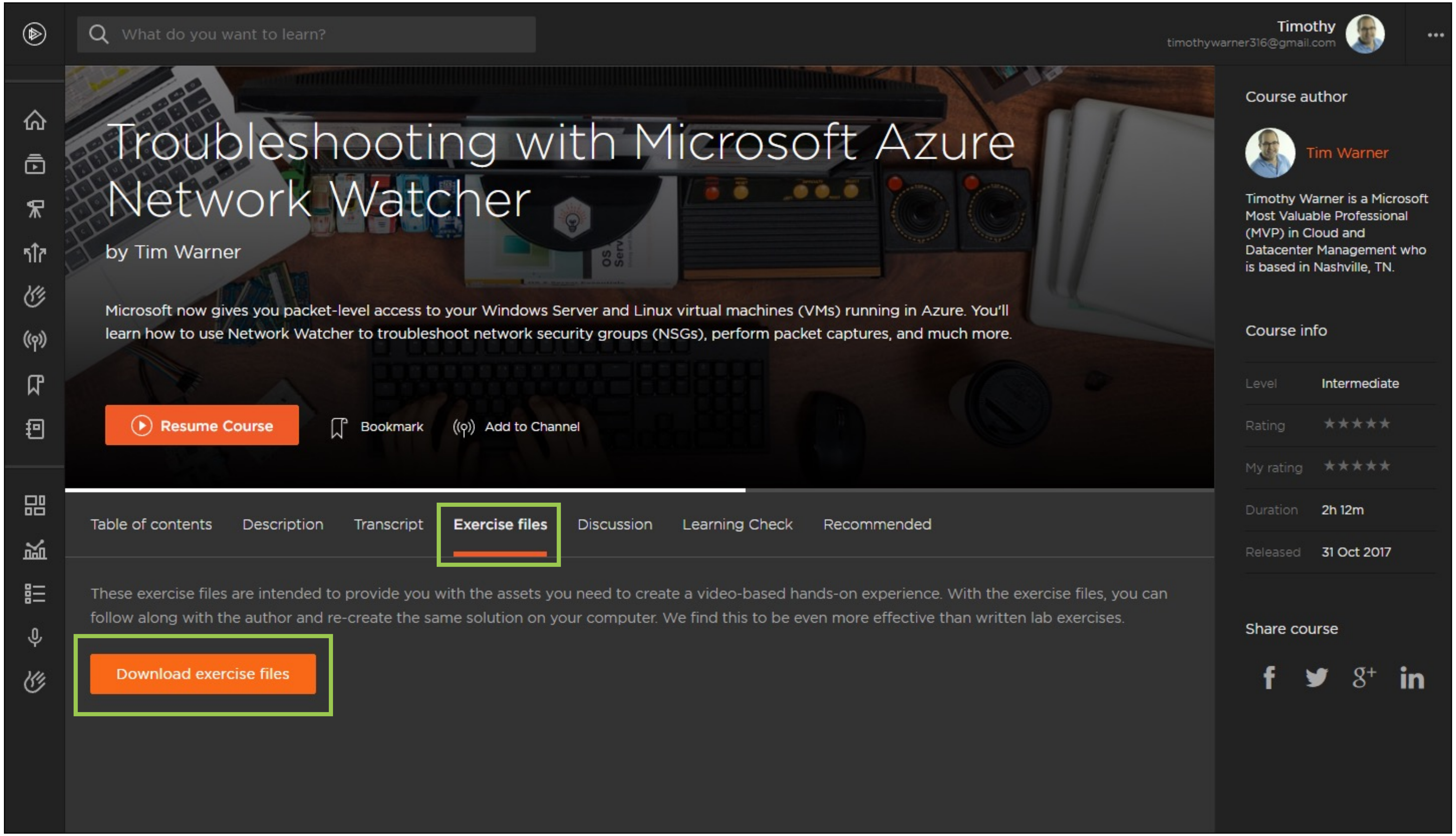
Design and Implement Routing (25–30%)

Design, implement, and manage VNet routing

- design and implement user-defined routes (UDRs)
- associate a route table with a subnet
- configure forced tunneling
- diagnose and resolve routing issues

timw.info/az700

Exercise Files



What do you want to learn?

Timothy
timothywarner316@gmail.com

Troubleshooting with Microsoft Azure Network Watcher

by Tim Warner

Microsoft now gives you packet-level access to your Windows Server and Linux virtual machines (VMs) running in Azure. You'll learn how to use Network Watcher to troubleshoot network security groups (NSGs), perform packet captures, and much more.

Resume Course | Bookmark | Add to Channel

Table of contents | Description | Transcript | **Exercise files** | Discussion | Learning Check | Recommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

Download exercise files

Course author

Tim Warner

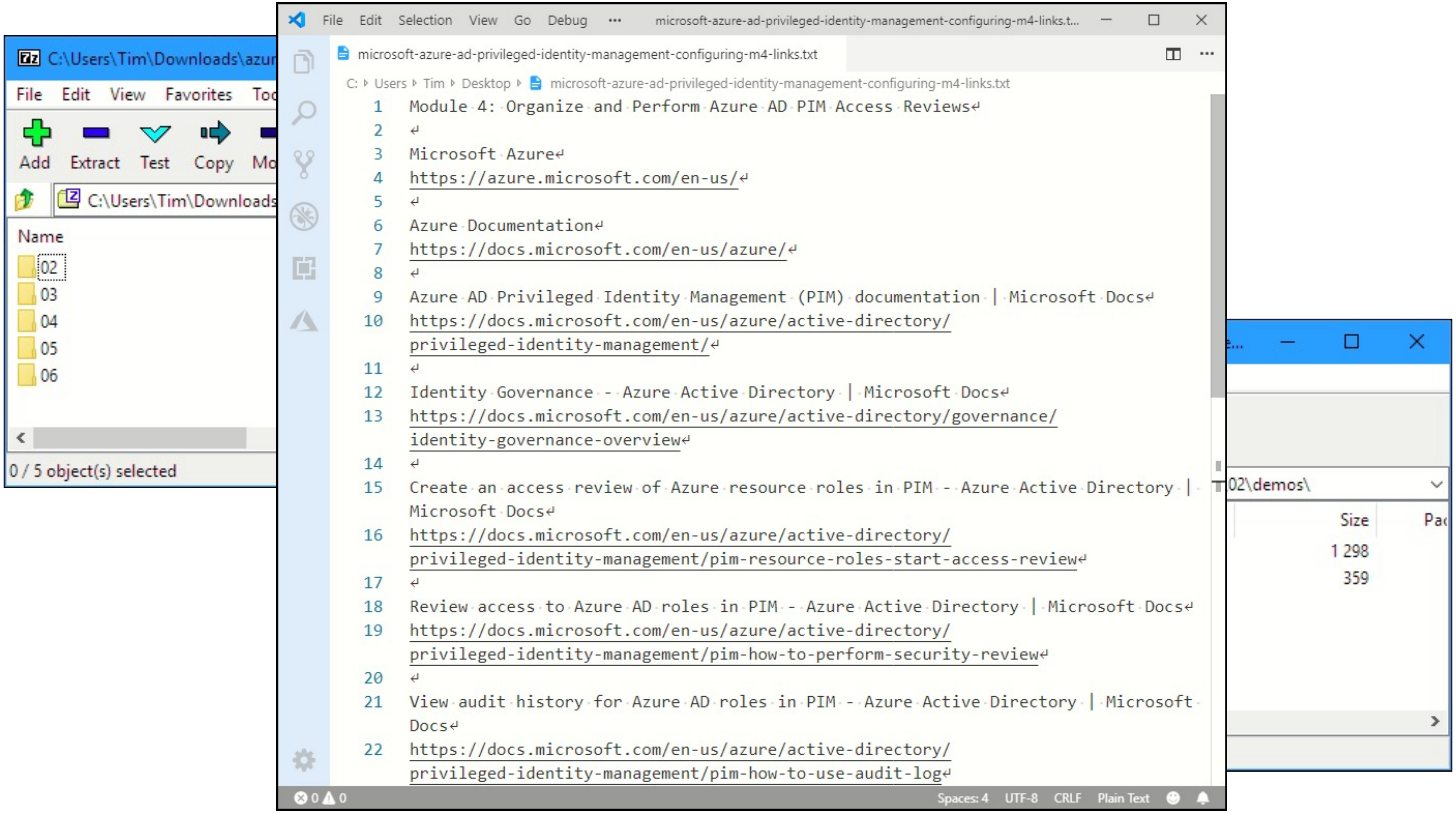
Timothy Warner is a Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management who is based in Nashville, TN.

Course info

Level	Intermediate
Rating	★★★★★
My rating	★★★★★
Duration	2h 12m
Released	31 Oct 2017

Share course

Exercise Files


C:\Users\Tim\Downloads\azur
File Edit View Favorites Too
Add Extract Test Copy Mo
C:\Users\Tim\Downloads
Name
02
03
04
05
06
0 / 5 object(s) selected
File Edit Selection View Go Debug ···
microsoft-azure-ad-privileged-identity-management-configuring-m4-links.t...
microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt
C: › Users › Tim › Desktop › microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt
ⓧ 0 ⚠ 0
Spaces: 4 UTF-8 CRLF Plain Text
e...
02\demos\
Size
Pa
1 298
359

```
Module 4: Organize and Perform Azure AD PIM Access Reviews

Microsoft Azure
https://azure.microsoft.com/en-us/

Azure Documentation
https://docs.microsoft.com/en-us/azure/

Azure AD Privileged Identity Management (PIM) documentation | Microsoft Docs
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/

Identity Governance - Azure Active Directory | Microsoft Docs
https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview

Create an access review of Azure resource roles in PIM - Azure Active Directory | Microsoft Docs
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review

Review access to Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-perform-security-review

View audit history for Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-use-audit-log
```

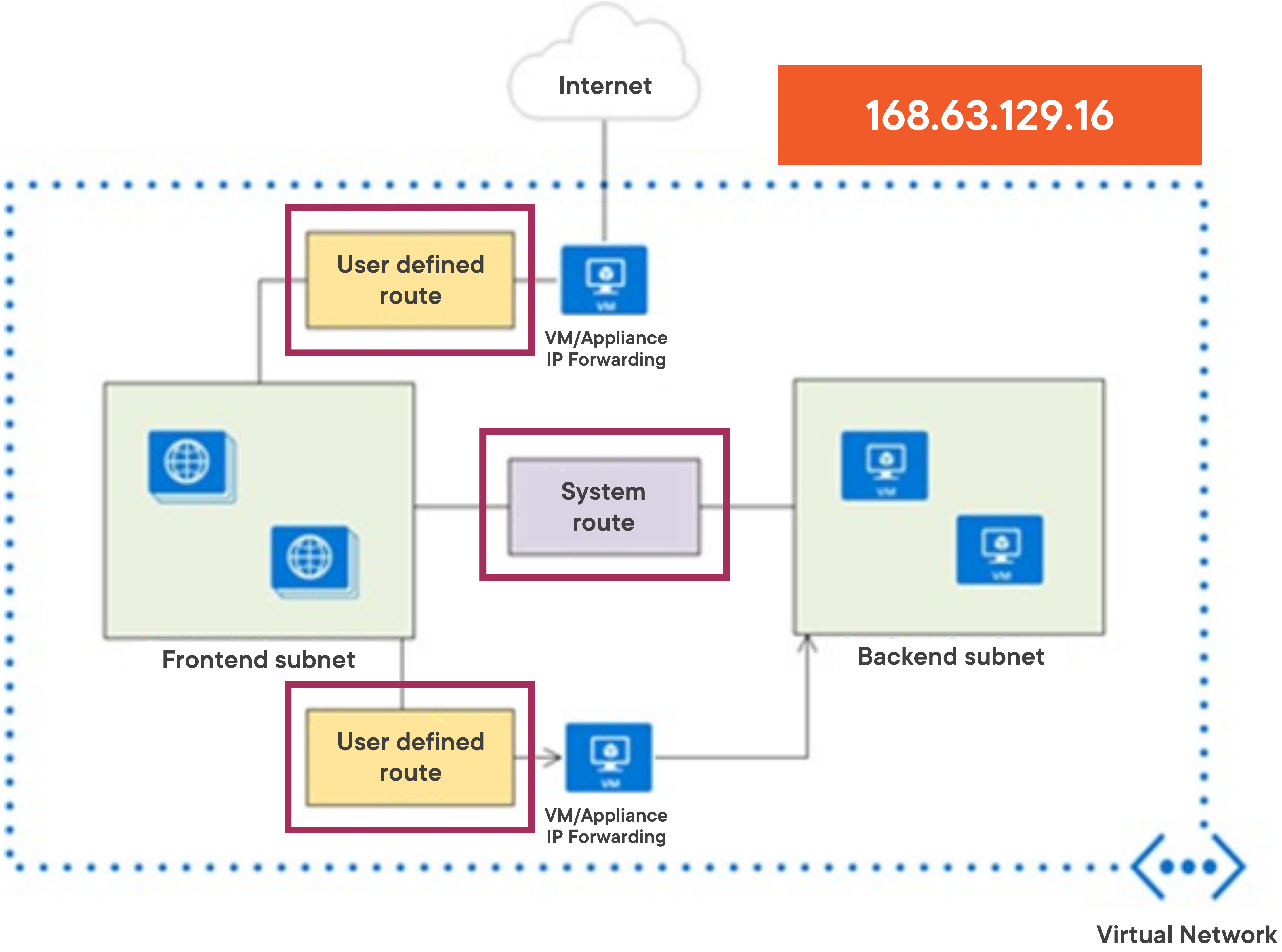
Implement User-Defined Routes

Azure System Routes

Can't delete

Can’t create

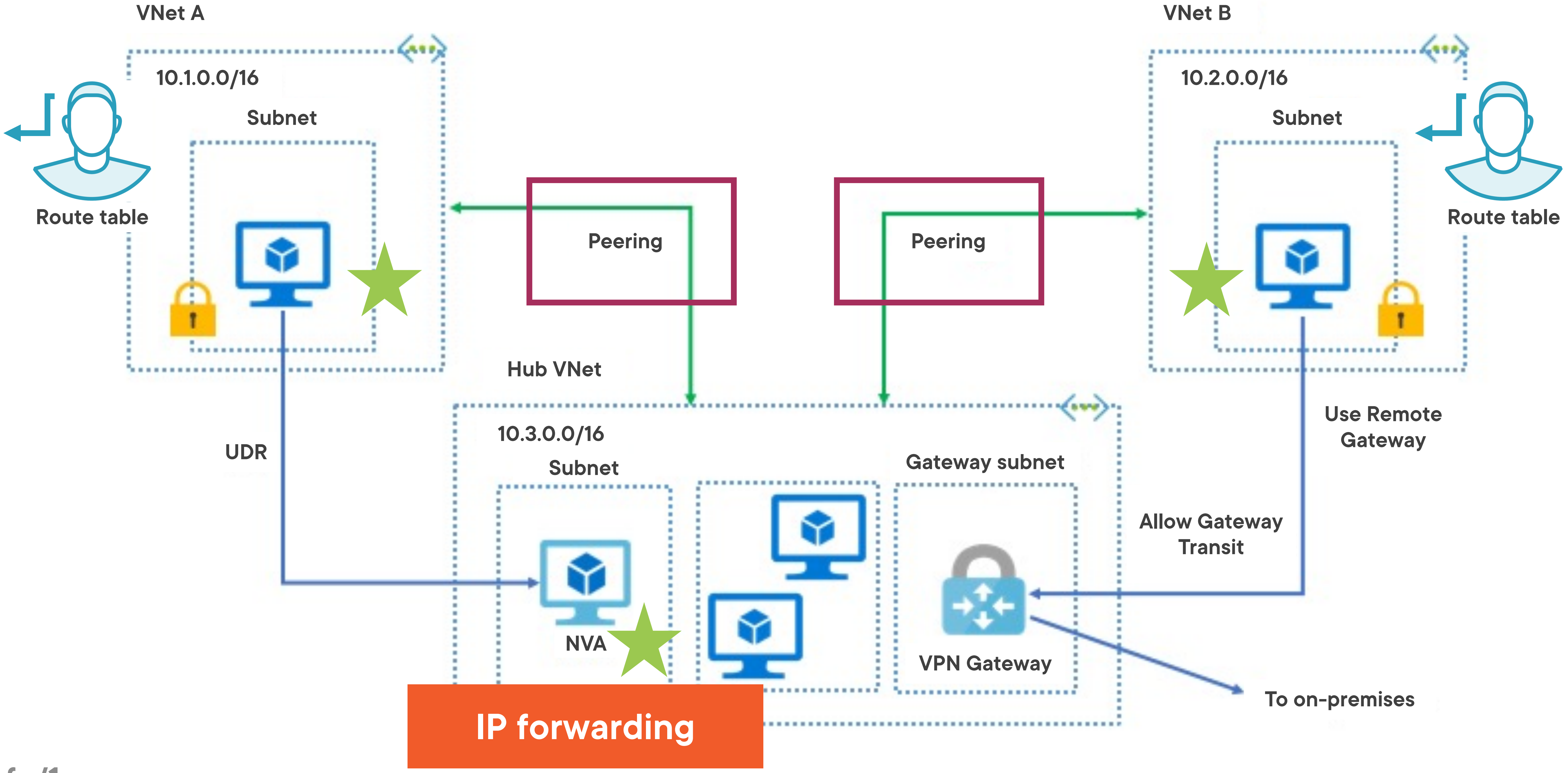
Can override



168.63.129.16

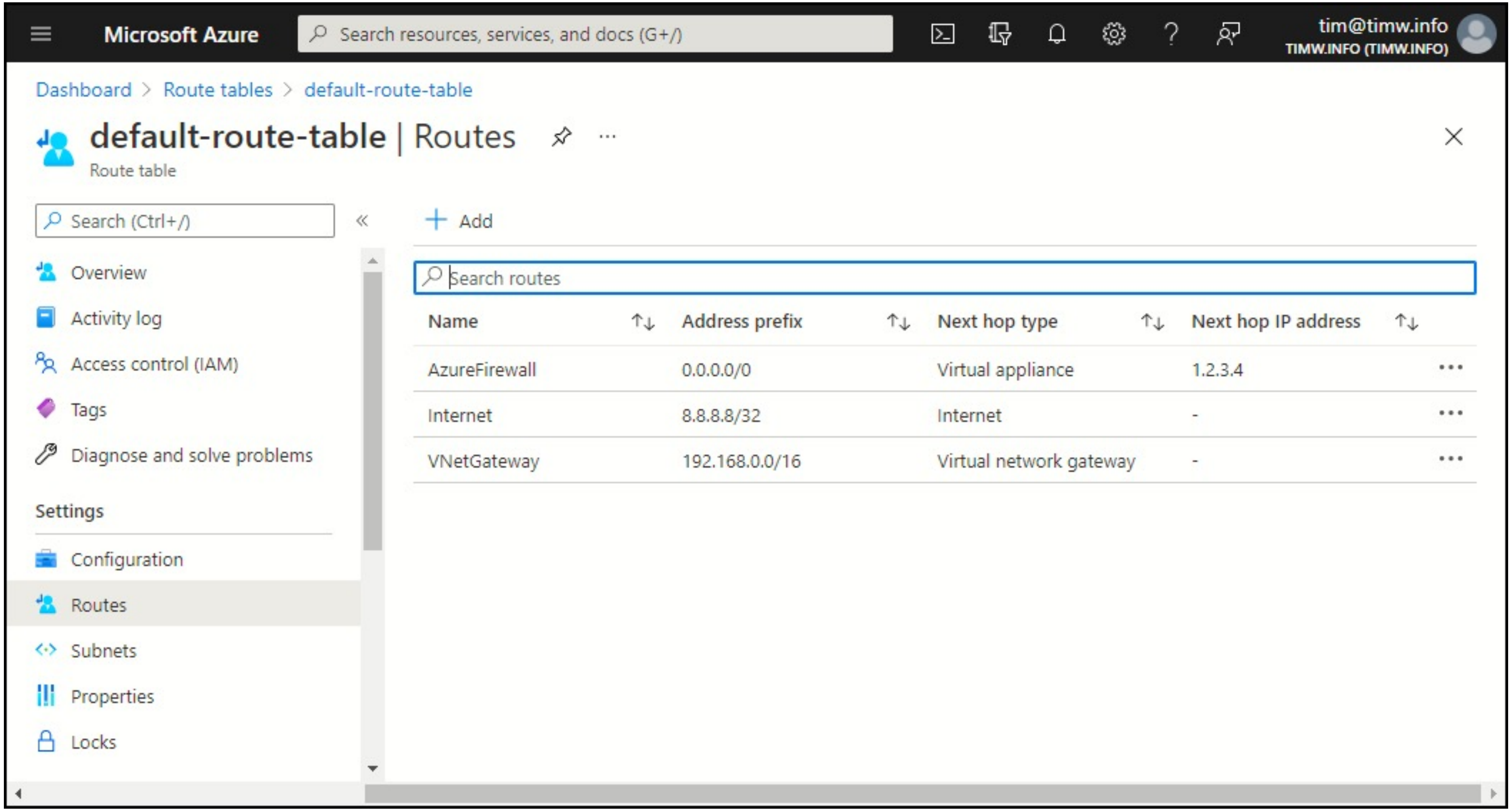
timw.info/0ag

Azure Hub-and-Spoke Architecture



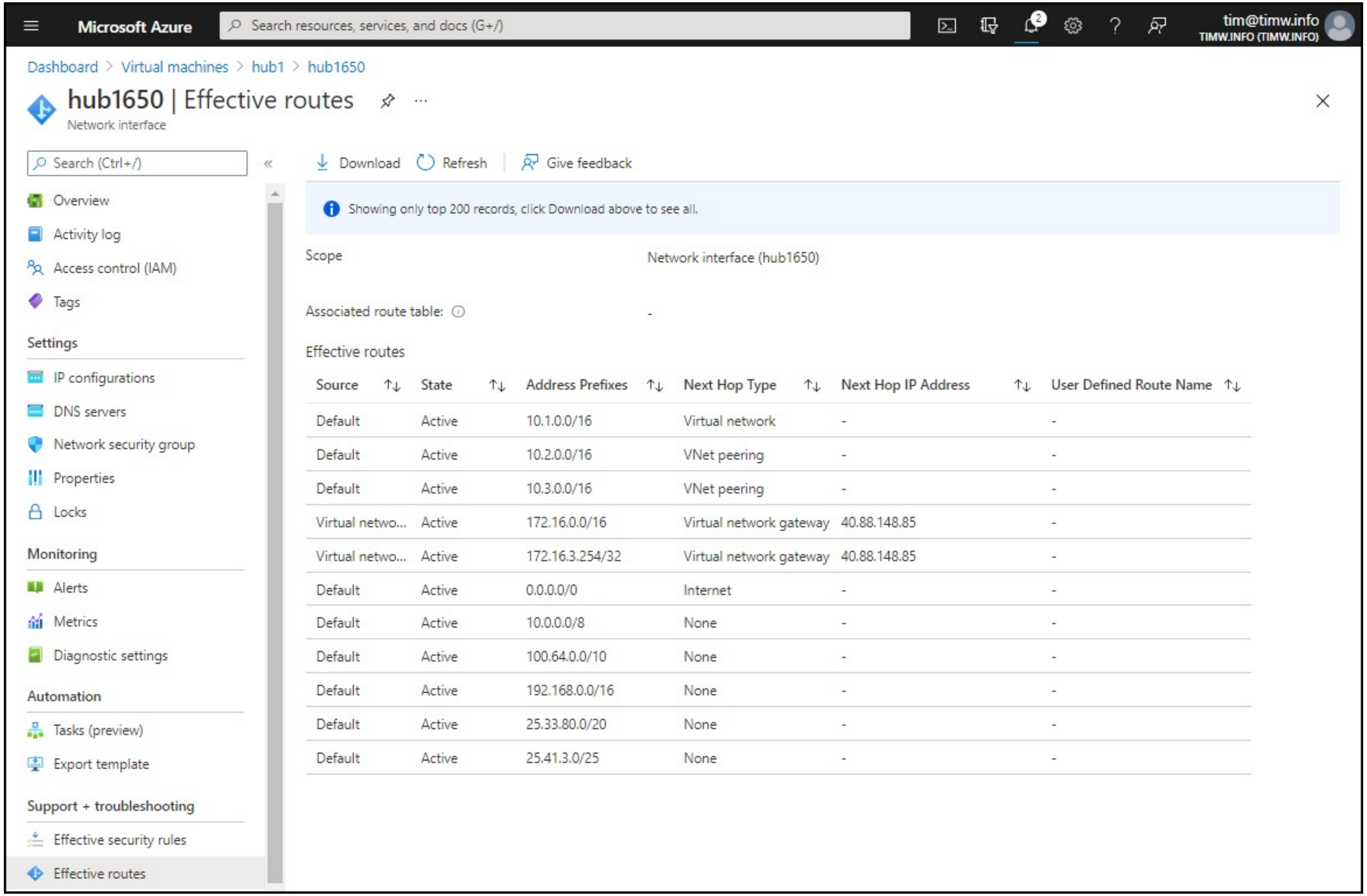
timw.info/1xv

Route Table



Name	Address prefix	Next hop type	Next hop IP address
AzureFirewall	0.0.0.0/0	Virtual appliance	1.2.3.4
Internet	8.8.8.8/32	Internet	-
VNetGateway	192.168.0.0/16	Virtual network gateway	-

Effective Routes



hub1650 | Effective routes

Network interface

Showing only top 200 records, click Download above to see all.

Scope: Network interface (hub1650)

Associated route table: -

Effective routes

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address	User Defined Route Name
Default	Active	10.1.0.0/16	Virtual network	-	-
Default	Active	10.2.0.0/16	VNet peering	-	-
Default	Active	10.3.0.0/16	VNet peering	-	-
Virtual netwo...	Active	172.16.0.0/16	Virtual network gateway	40.88.148.85	-
Virtual netwo...	Active	172.16.3.254/32	Virtual network gateway	40.88.148.85	-
Default	Active	0.0.0.0/0	Internet	-	-
Default	Active	10.0.0.0/8	None	-	-
Default	Active	100.64.0.0/10	None	-	-
Default	Active	192.168.0.0/16	None	-	-
Default	Active	25.33.80.0/20	None	-	-
Default	Active	25.41.3.0/25	None	-	-

How Azure Selects Routes

Prefix length

- 10.0.0.0/24 is preferred over 10.0.0.0/16 due to longer prefix

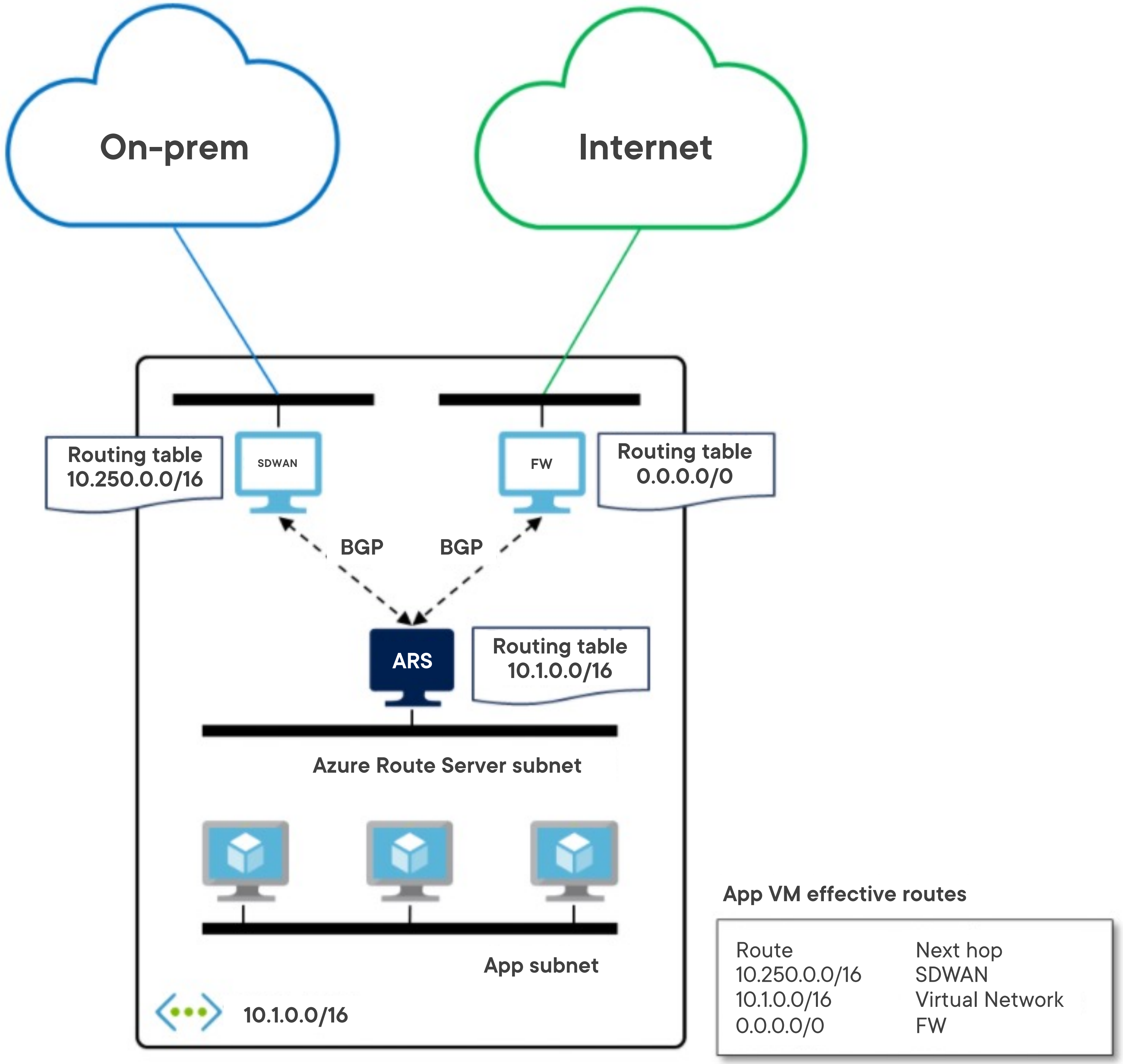
Example

- 10.0.0.5 (exact match)
- For destination 10.0.1.5, 10.0.0.0/16 would be chosen over 10.0.0.0/24

Multiple routes w/ same prefix

1. User-defined route
2. BGP route
3. System route

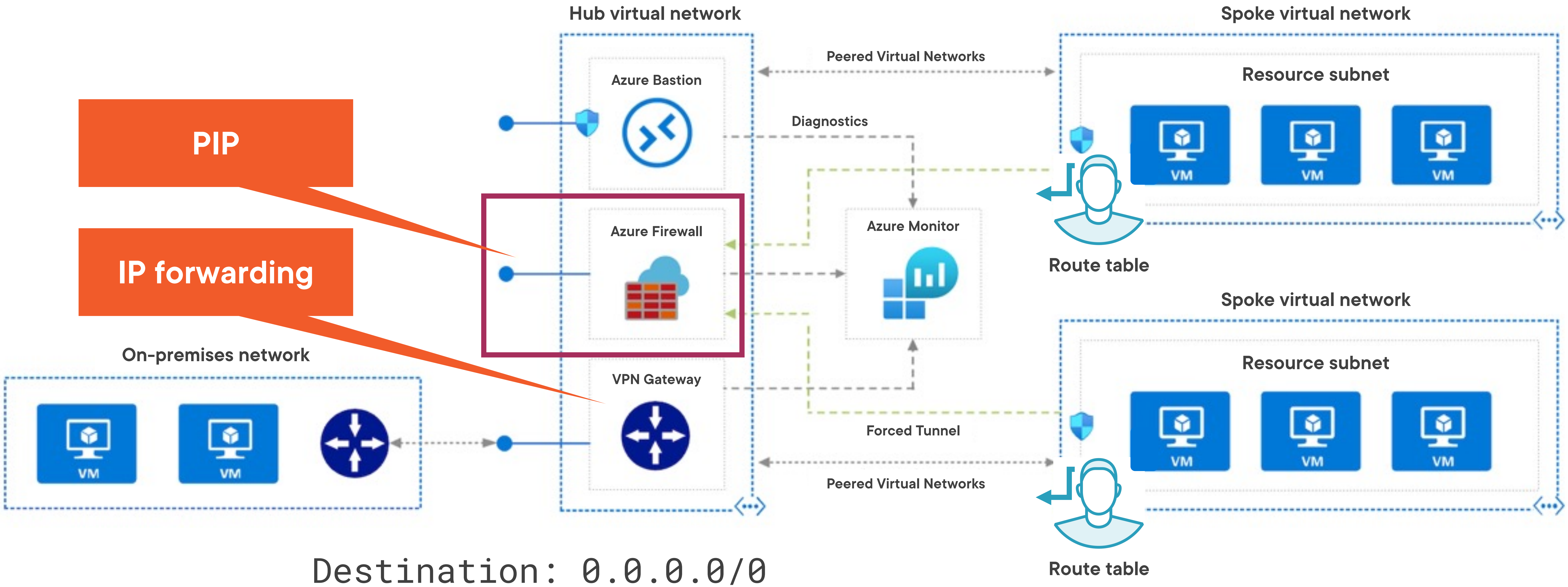
Azure Route Server



Route	Next hop
10.250.0.0/16	SDWAN
10.1.0.0/16	Virtual Network
0.0.0.0/0	FW

- Public Preview as of Fall 2021
- Simplifies dynamic routing between your NVA(s) and your VNets
- Border Gateway Protocol (BGP)
- Azure VNet Gateway and ExpressRoute are supported
- Third-party NVAs

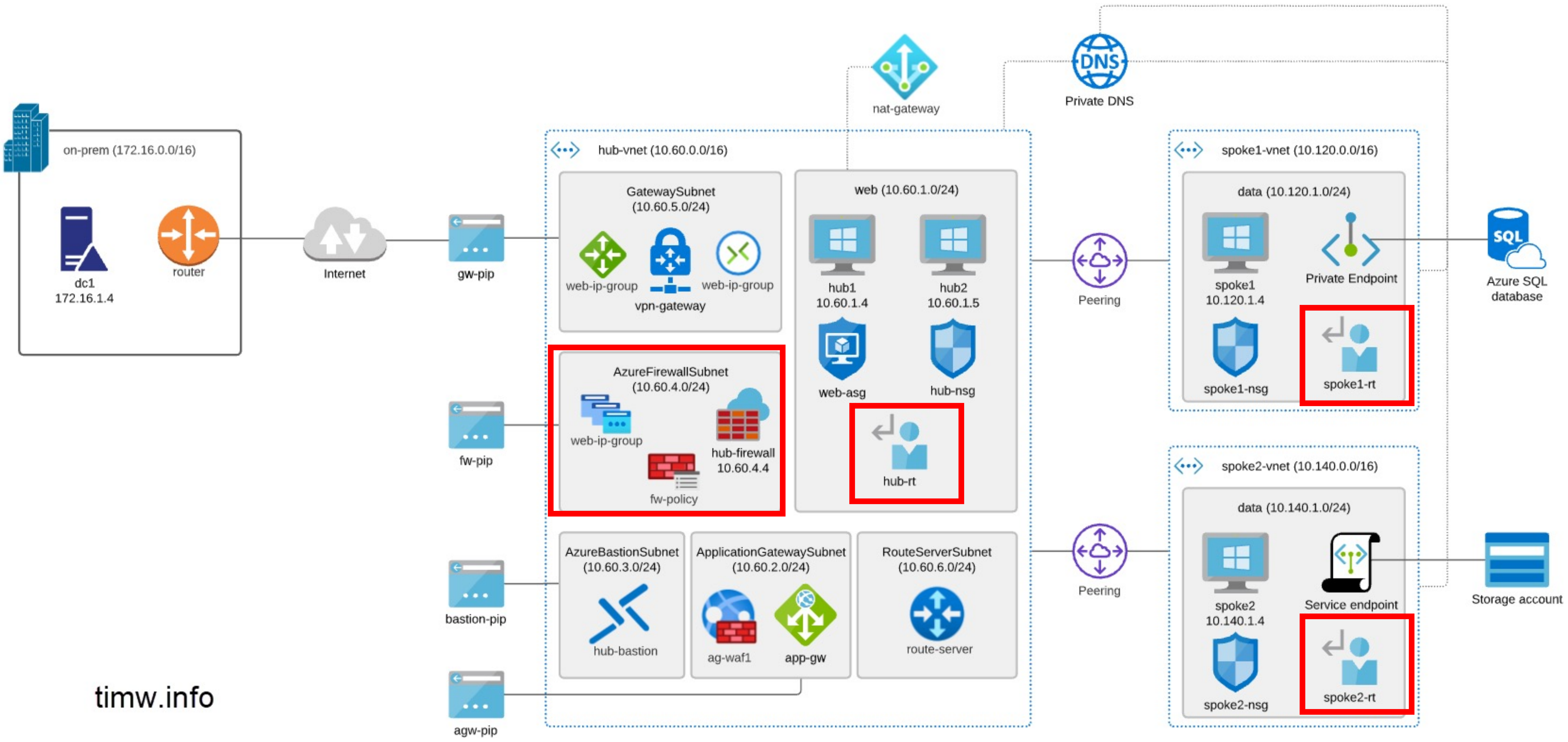
Example: Azure Firewall Deployment



```
Destination: 0.0.0.0/0
Next Hop: Virtual appliance
```

timw.info/d4f

Our Lab Environment



timw.info

Demo

1

Deploy Azure Firewall

Configure routes

Create quick WWW policy

Test access

Configure Forced Tunneling

What is Forced Tunneling?

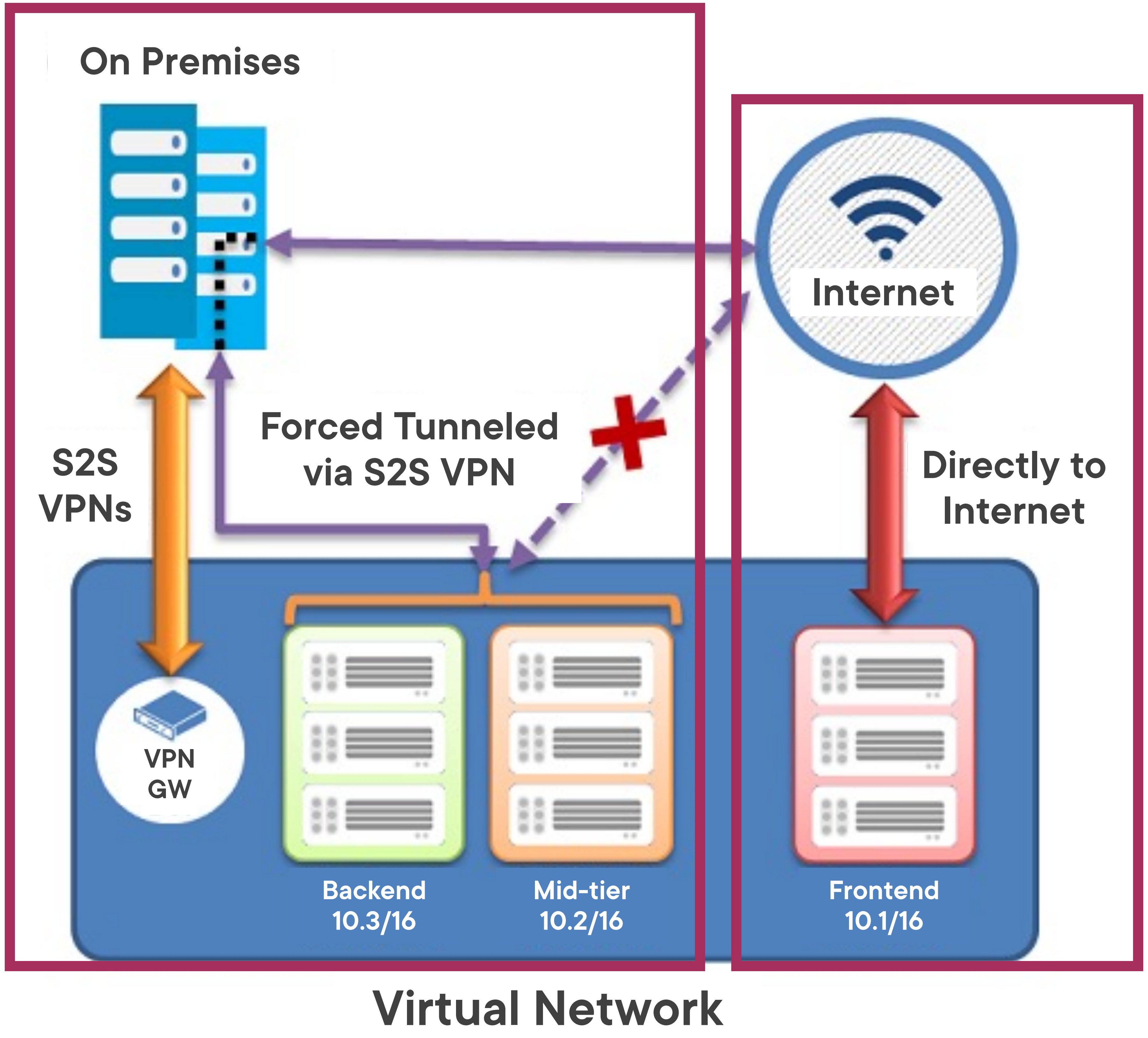
Concept that applies to S2S VPN, ExpressRoute, and Azure Firewall

Redirect Internet-bound traffic back to your on-premises location

- Inspection and auditing

Configured via Azure PowerShell

Forced Tunneling - Azure VPN



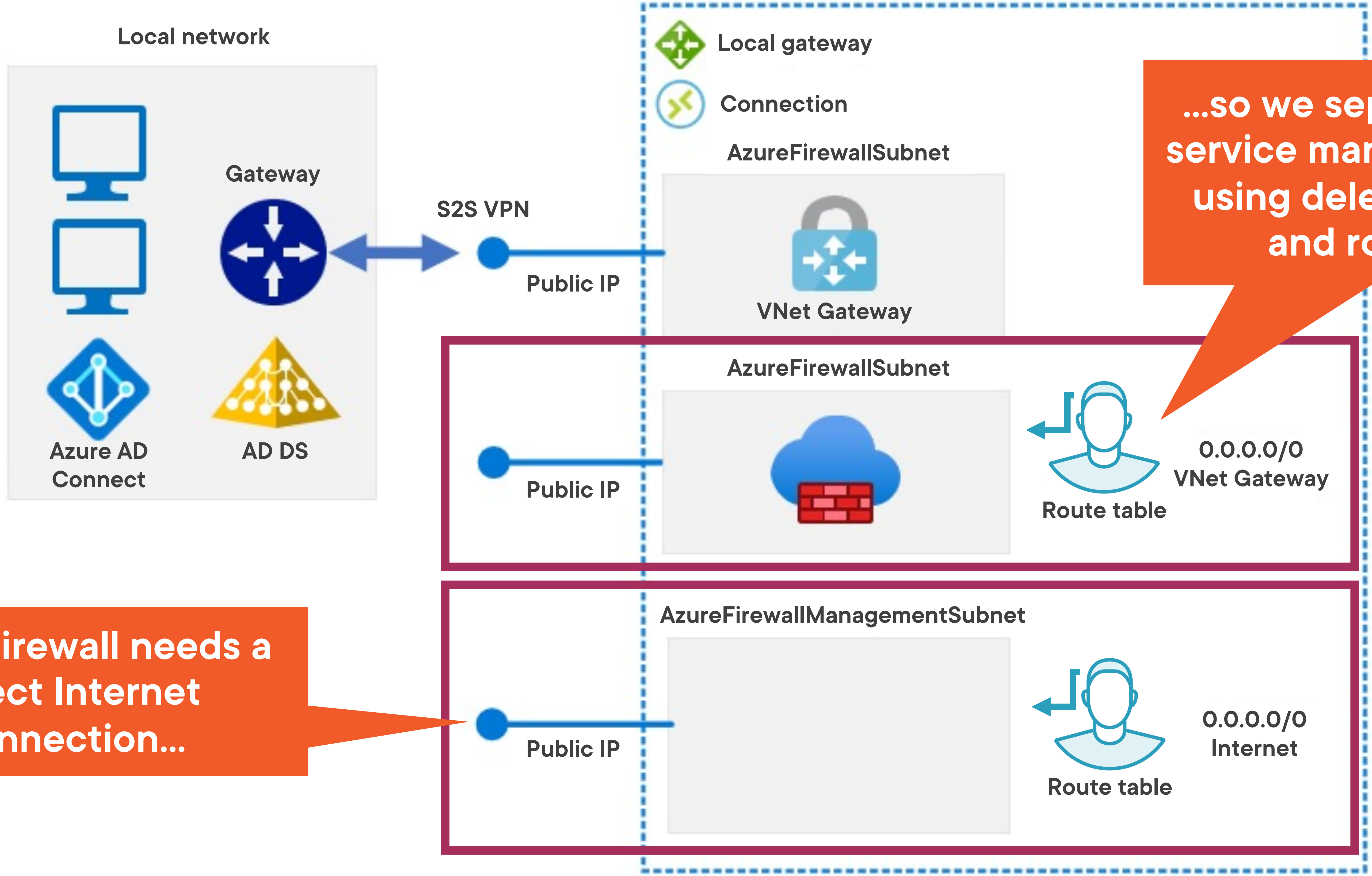
Azure S2S VPN Forced Tunneling Configuration

```
$LocalGateway = Get-AzLocalNetworkGateway -Name "DefaultSiteHQ"
  -ResourceGroupName "ForcedTunneling"

$VirtualGateway = Get-AzVirtualNetworkGateway -Name "Gateway1"
  -ResourceGroupName "ForcedTunneling"

Set-AzVirtualNetworkGatewayDefaultSite
  -GatewayDefaultSite $LocalGateway
  -VirtualNetworkGateway $VirtualGateway
```

Forced Tunneling - Azure Firewall



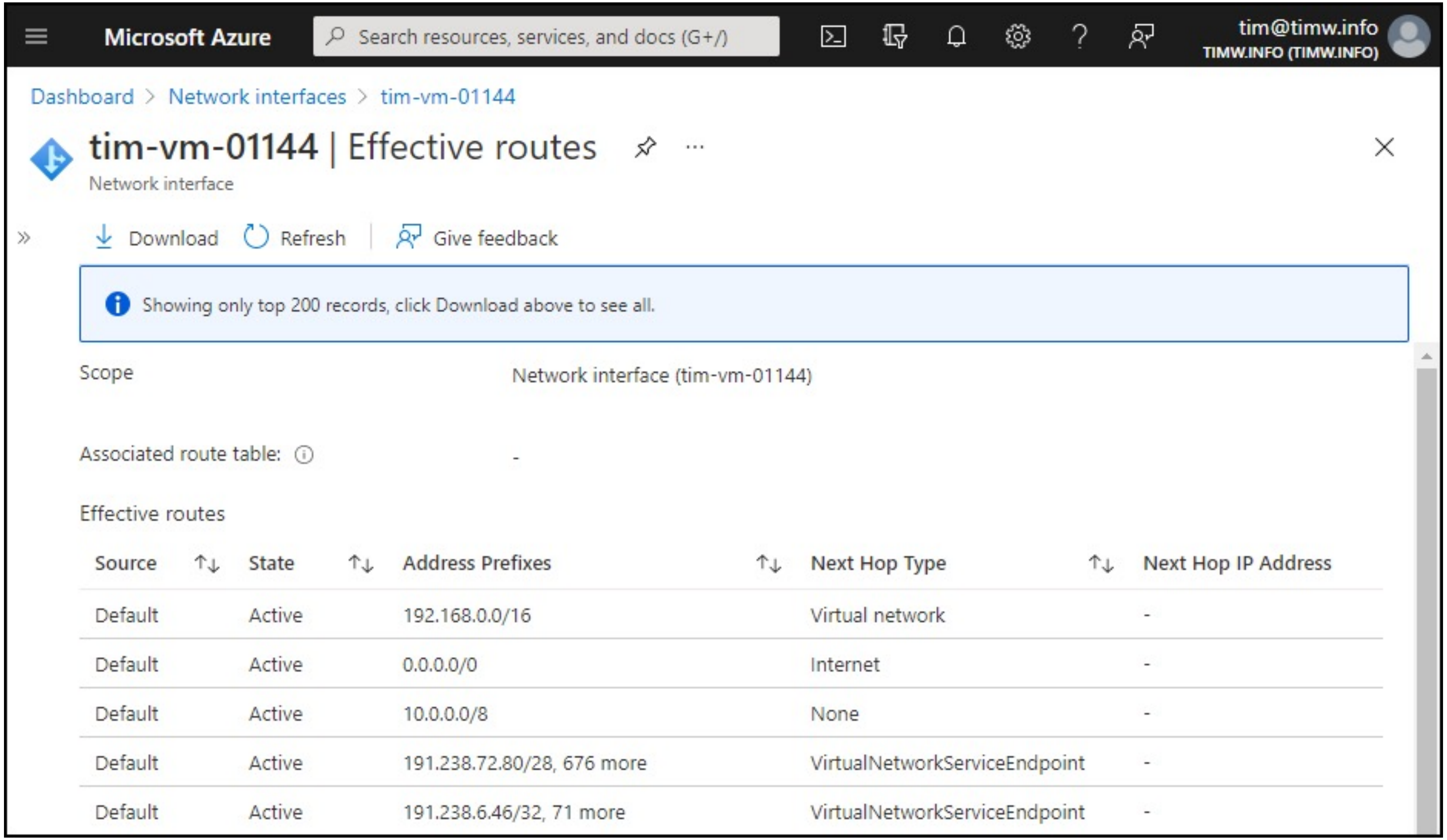
…so we separate user and service management traffic using delegated subnets and route tables

Azure Firewall needs a direct Internet connection…

timw.info/fwt

Diagnose and Resolve Routing Issues

Azure VM NIC Effective Routes


Microsoft Azure
Search resources, services, and docs (G+/)
tim@timw.info
TIMW.INFO (TIMW.INFO)
Dashboard > Network interfaces > tim-vm-01144
Download
Refresh
Give feedback

tim-vm-01144 | Effective routes

Network interface

Showing only top 200 records, click Download above to see all.

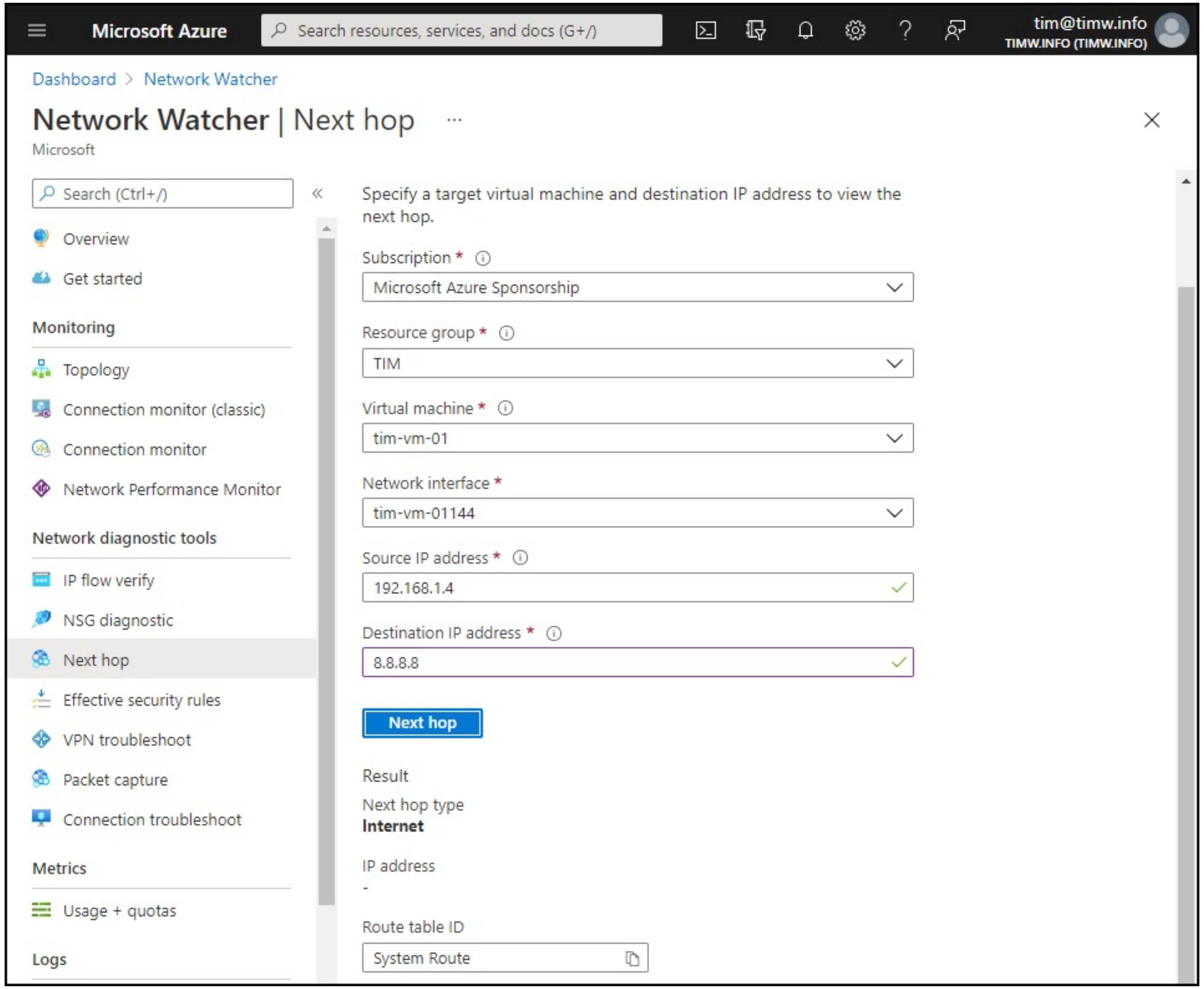
Scope: Network interface (tim-vm-01144)

Associated route table: -

Effective routes

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	192.168.0.0/16	Virtual network	-
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	191.238.72.80/28, 676 more	VirtualNetworkServiceEndpoint	-
Default	Active	191.238.6.46/32, 71 more	VirtualNetworkServiceEndpoint	-

Network Watcher: Next Hop



Microsoft Azure
Search resources, services, and docs (G+/)
tim@timw.info
TIMW.INFO (TIMW.INFO)
Dashboard > Network Watcher

Network Watcher | Next hop

Microsoft

Specify a target virtual machine and destination IP address to view the next hop.

Subscription * : Microsoft Azure Sponsorship

Resource group * : TIM

Virtual machine * : tim-vm-01

Network interface * : tim-vm-01144

Source IP address * : 192.168.1.4

Destination IP address * : 8.8.8.8

Next hop

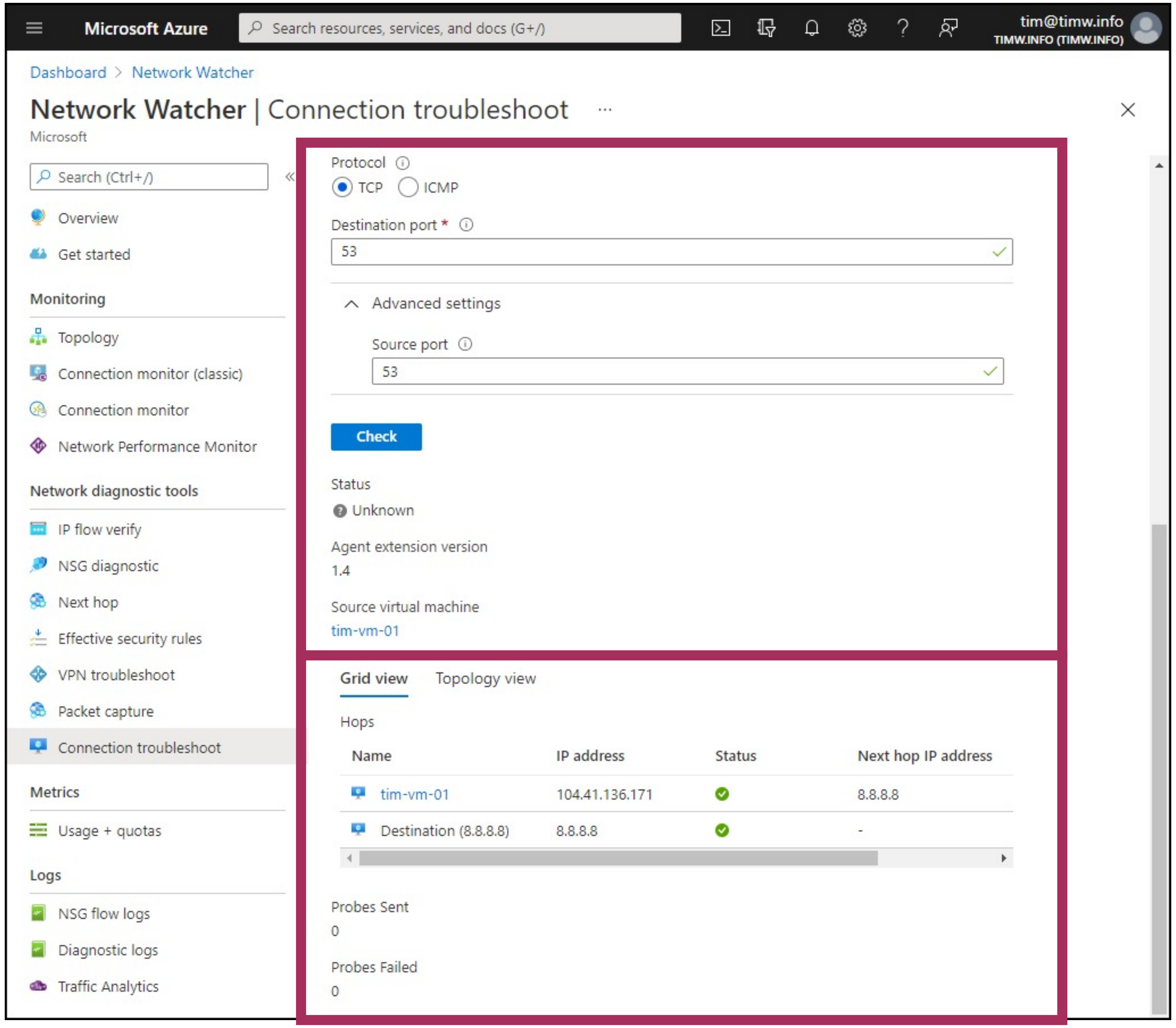
Result

Next hop type
Internet

IP address
-

Route table ID
System Route

Network Watcher: Connection Troubleshoot



Network Watcher | Connection troubleshoot

Microsoft

Protocol ⓘ

● TCP ○ ICMP

Destination port * ⓘ

53

Advanced settings

Source port ⓘ

53

Status

Unknown

Agent extension version

1.4

Source virtual machine

tim-vm-01

Hops

Name	IP address	Status	Next hop IP address
tim-vm-01	104.41.136.171	✓	8.8.8.8
Destination (8.8.8.8)	8.8.8.8	✓	-

Probes Sent

0

Probes Failed

0

Demo

2

Effective routes

Network Watcher

- Next Hop
- Connection troubleshoot

Configure Azure Firewall forced tunneling

Summary

Azure system routing offers great convenience

You are ultimately in control of your Azure routing paths

Keep an eye out for Azure Route Server

Up Next:
Design and Implement an Azure Load Balancer